Vysoká Škola Báňská – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Možnosti zabezpečených datových přenosů v bezdrátových sítích

Possibilities security data transmission in Wireless networks

2009
VŠB – Technická univerzita Ostrava
Katedra informatiky

Jakub Hargaš
Fakulta elektrotechniky a informatiky
Akademický rok 2008/2009

Zadání bakalářské práce

Student: **Jakub Hargaš**

Studijní program: B2647 Informační a komunikační technologie

Studijní obor: 2612R059 Mobilní technologie

Téma: Možnosti zabezpečených datových přenosů v bezdrátových sítích

Possibilities security data transmission in Wireless networks

Zásady pro vypracování:

Přenos dat v bezdrátových sítích představuje velké bezpečnostní rizika. V rámci řešení bakalářské práce se seznamte s problematikou bezpečnostních rizik a navrhněte a ověřte jednotlivé metody zabezpečení.

1. Seznamte se s problematikou bezpečných přenosů v bezdrátových sítích.
2. Graficky zpracujte tuto problematiku pomocí www stránek a Macromedia FLASH.
3. Navrhněte a ověřte bezdrátové datové přenosy v laboratoři.

Seznam doporučené odborné literatury:

Podle pokynů vedoucího bakalářské práce.

Formální záležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce**: Ing. Pavel Nevlud**

Datum zadání: 30.11.2008
Datum odevzdání: 07.05.2009

doc. Dr.Ing. Eduard Sojka	prof. Ing. Ivo Vondrák, CSc.
vedoucí katedry	*děkan fakulty*

Rád bych na tomto místě poděkoval Ing. Pavlu Nevludovi za návrh tématu práce, poskytnutí školní laboratoře a za následné komentáře. Taktéž bych zde chtěl poděkovat Ondřeji Pavelkovi, poskytovateli bezdrátového internetu – firmě OpeNET (www.openet.cz), za zapůjčení hardware pro otestování různých metod zabezpečení.

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě dne 07. 05. 2009 ……

Jakub Hargaš

Abstrakt

Práce popisuje možnosti zabezpečení bezdrátových sítí. Zabývá se hlavně zabezpečením sítí standardu IEEE 802.11. Jelikož však zabezpečení v tomto původním standardu se ukázalo jako nedostatečné, srovnává a popisuje tato práce i později vzniklé bezpečnostní doplňky k tomuto standardu. Práce popisuje jednotlivé principy autentizace, šifrování a integrity přenášených dat pro různé typy zabezpečení. Poukazuje na výhody a nevýhody při použití určitých zabezpečovacích metod, následně tyto popisované metody ukazuje i na příkladech konfigurací. V závěru práce je pak navrženo zabezpečení typických síťových infrastruktur, jako je síťová topologie poskytovatele internetu, firmy nebo domácnosti, popřípadě malé kanceláře. Následně je tato problematika graficky zpracována i jako příloha ve formě www stránek a technologie Macromedia FLASH.

Klíčová slova

Wi-Fi, bezpečnost, bezdrátová síť, IEEE 802.11, WEP, WPA, IEEE 802.11i, WPA2, RADIUS, EAP

Abstract

The work describes the possibilities of securing wireless networks. It deals mainly with the network security standard IEEE 802.11. However, security in the original standard was inadequate; this work describes and compares security add-ons to this standard. The work describes the principles of authentication, encryption and integrity of transmitted data for different types of security. It refers to the advantages and disadvantages in the use of certain methods of protection, then the described methods are shown on examples of configurations. In conclusion, the work is proposed to typical network security infrastructures, such as network topology ISP, company or household, where appropriate, small offices. Consequently, this issue is design as a supplement in the form of web pages and Macromedia FLASH technology.

Keywords

Wi-Fi, security, wireless network, IEEE 802.11, IEEE 802.1x, WEP, WPA, IEEE 802.11i, WPA2, RADIUS, EAP

Seznam použitých symbolů a zkratek

AAA server	(Authentication, Authorization and Accounting Server) – Server zajišťující autentizaci, autorizaci a účtování. Tuto funkci může plnit například RADIUS server.
AES	(Advanced Encryption Standard) – Šifrovací standard vyvinutý v roce 2000.
AP	(Acces Point) – V kontextu této práce vnímán jako bezdrátový přístupový bod.
ASCII	(American Standard Code for Information Interchange) – Kódová tabulka která definuje znaky anglické abecedy, a jiné znaky používané v informatice.
DoS	(Denial of Service) – Útok vedoucí k odmítnutí služby. Zamezení oprávněnému uživateli využívat síťových služeb.
EAP	(Extensible Authentication Protocol) – Autentizační rámec podporující různé autentizační mechanismy. Využívá ho standard IEEE 802.1x.
IEEE	(Institute of Electrical and Electronics Engineers) Institut pro elektrotechnické a elektronické inženýrství.
ICV	(Integrity Check Value) Hodnota používaná pro ověření integrity dat.
IV	(Initialization Vector) Inicializační vektor.
LAN	(Local Area Network) Síť lokálního nebo místního charakteru.
MAC adresa	(Media Access Control) Jedinečný identifikátor síťového zařízení, který používají různé protokoly druhé (spojové) vrstvy OSI.
MIC	(Message Integrity Check) Hodnota používaná pro ověření integrity dat.
PMK	(Pairwise Master Key) Šifrovací klíč, dle něhož se odvozují další klíče nižší úrovně.
PRNG	(Pseudorandom Number Generator) Pseudonáhodný generátor generující sekvenci bitů o délce dat a ICV
RC4	(Ron's Code No. 4) Symetrická proudová šifra vyvinutá roku 1987 Ronaldem Riverstem [3].
SSID	(Service Set IDentifier) Jmenný identifikátor bezdrátové sítě.
TKIP	(Temporal Key Integrity Protocol) Protokol pro šifrování dynamickým klíčem.
WEP	(Wired Equivalent Privacy) Zabezpečení bezdrátových sítí dle původního standardu IEEE 802.11 kladoucí si za cíl srovnatelné bezpečnosti s drátovými sítěmi.

Obsah

1 Úvod

Technologie bezdrátového přenosu dat se v posledních letech dynamicky rozvíjejí, jelikož přinášejí značnou míru pohodlí a mobility uživatelům těchto sítí. Stejně tak budování bezdrátové sítě může být ekonomicky výhodnější, přičemž přenosové rychlosti se v závislosti na použitých zařízeních mohou blížit sítím LAN. Taktéž se tyto sítě nasazují i jako technologie poslední míle, hlavně díky své dostupnosti, ačkoli nebyly takto původně koncipovány.

Jelikož však bezdrátové sítě šíří svá data pomocí rádiových signálů, je zde na rozdíl od drátových technologií, např. jako je Ethernet, složitější řízení a kontrola přístupu. Zatímco s drátovou síti je nutno mít fyzický přístup k síťovému portu, tak při použití bezdrátových řešení toho odpadá, a je zde možnost se připojit k síti z jakéhokoli místa, do kterého zasahuje rádiový signál dané bezdrátové sítě. Rozdíl mezi bezdrátovou a drátovou sítí je porovnán níže:

- Prostředí drátových sítí lze považovat za soukromé. Předpokládá se zde, že neautorizovaný uživatel se nemůže fyzicky připojit k síťovému portu, a tak se nemusíme starat, kdo se připojuje. Data jsou přenášená síťovým kabelovým systémem, tím pádem jsou utajená proti odposlechu neautorizovaným uživatelem.
- Prostředí bezdrátových sítí lze považovat za veřejné. Každý uživatel s kompatibilními nástroji se může pokusit připojit. Je zde tedy nutno zajistit co nejvyšší míru ochrany proti přístupu neautorizovaných uživatelů, stejně tak jako utajení přenášených dat uvnitř sítě.

Zabezpečení bezdrátových sítí a jejich možnosti se tak stávají jedním z klíčových elementů této technologie. Hlavní aspekty bezpečnosti bezdrátových sítí se skládají z těchto prvků:

- **Autentizace** Dříve než je uživateli umožněno přenášet sítí data, je nutno samotného uživatele věrohodně identifikovat, k čemuž se používají různé autentizací metody, které budu popisovat v následujících kapitolách.
- **Šifrování** Dříve, než se odešle do sítě datový paket, musí být jeho obsah zašifrován pro zajištění dostatečného utajení přenášených dat.
- **Integrita dat** Integritou přenášených dat je myšleno zajištění neměnnosti datového paketu od jeho odesláni, do jeho doručení. Dříve, než se vyšle do bezdrátové sítě datový paket, musí být k němu přiložena informace, podle které může přijímač rozeznat neměnnost a úplnost paketu.

V současné době mají bezdrátové sítě pevné místo v domácnostech i ve firmách. Zabezpečení domácích sítí je však často na nevalné úrovni, snad díky instalaci uživateli s minimálními znalostmi této problematiky. Nezřídka kdy se stává, že zařízení jsou ponechána ve výchozím nastavení, které bývá většinou bez jakéhokoli zabezpečení. U firem, pokud má správce dobrý přehled o zásadách zabezpečení bezdrátových sítí, je často situace lepší. Nicméně, dobrá znalost těchto zásad je jednou z nejdůležitějších deviz, jak při zabezpečení sítě podniku, tak i jako součást bezpečnostní politiky podniku celkově.

Ve své práci jsem se rozhodl vybrat si několik metod zabezpečení a ty ukázat prakticky i s popisem konfigurace. Z bezdrátových síťových technologií jsem si vybral technologie podle standardu IEEE 802.11, jelikož jsou široce rozšířené, mají, na rozdíl od jiných bezdrátových technologií, jako je

kupříkladu Bluetooth, výrazně vyšší dosah, útočník nepotřebuje drahý hardware pro připojení, odposlech dat nebo narušení požadované funkcionality zavedené síťové topologie. Roste tak zde důraz na zabezpečení snad více, než kde jinde.

Pokud není uvedeno jinak, při použití softwarových AP jsem využil pro jejich konfiguraci operačního systému Linux, konkrétně distribuce Debian ve verzi 5.0.1 (Lenny).

2 Problematika bezpečných bezdrátových přenosů

Jak popisuji v úvodu, budu v této práci rozebírat hlavně bezpečnost bezdrátových sítí pracujících na frekvenci 2.4GHz – tzv. Wi-Fi. Právě řešení bezpečnosti těchto sítí je velice důležité, a to ať už z hlediska masivního nasazení ve firmách nebo podnicích, ale i z toho hlediska, že tyto sítě, původně navržené jako lokální, se dnes používají i jako technologie přenosu dat poslední míle u různých poskytovatelů internetu. Wi-Fi sítě totiž charakterizuje velice dobrá dostupnost, jak z hlediska finančního, tak i z hlediska informačního.

2.1 Možnosti zabezpečených datových přenosů v sítích standardu IEEE 802.11

Původní standard IEEE 802.11 definoval autentizaci, šifrování a integritu přenášených dat. Jak se však později ukázalo, původní návrh zabezpečení bezdrátové sítě založené na tomto standardu byl docela slabý, těžkopádný a proto velice neefektivní pro nasazení ve složitějších síťových infrastrukturách. Proto byl časem tento standard rozšířen, aby splňoval zvýšené požadavky na bezpečnost a aby byl efektivnější z hlediska časové složitosti konfigurace.

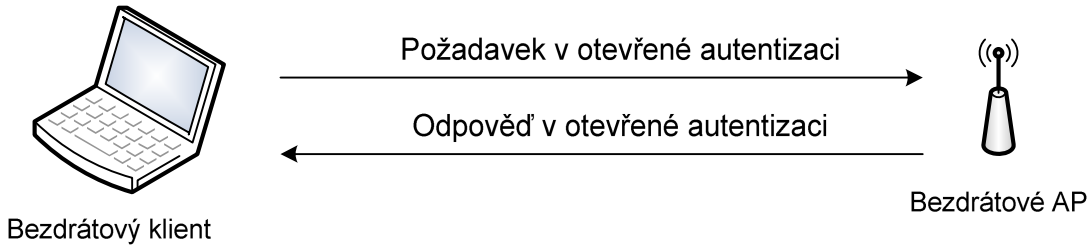
2.1.1 Autentizace

Standard IEEE 802.11 rozlišuje dva typy autentizace:

- Otevřená autentizace
- Autentizace na základě sdíleného klíče

2.1.1.1 Otevřená autentizace

Otevřená autentizace není založena na prověřování identifikačních údajů klienta, pouze identifikuje MAC adresu zařízení snažícího se připojit do sítě. Tento typ autentizace se používá v případech, kdy není žádná autentizace ve skutečnosti vyžadována. Proces otevřené autentizace je zobrazen níže (obr. 1):



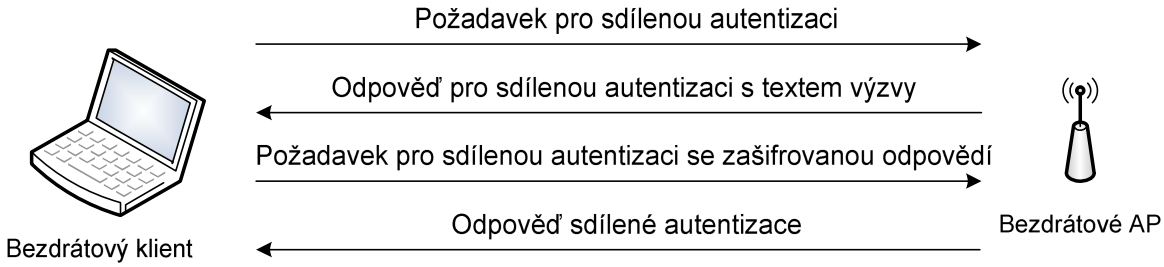
Obr. 1: Průběh otevřené autentizace

1. Bezdrátový klient, který se pokouší autentizovat vůči bezdrátové síti, vyšle autentizací rámec 802.11, který obsahuje jeho identifikační údaje, těmi jsou zdrojová MAC adresa a zdrojová IP adresa vyslaného rámce 802.11.
2. Příjemce, typicky bezdrátové AP, poskytne odpověď se zprávou úspěchu nebo neúspěchu, zda se podařilo bezdrátového klienta autentizovat.

2.1.1.2 Autentizace na základě sdíleného klíče

Při autentizaci sdíleným klíčem si AP ověřuje vůči žadateli o autentizaci (bezdrátovému klientu) znalost sdíleného klíče, který je statický a stejný pro všechny klienty dané sítě. Jednou ze slabin této

autentizační metody je, že se neověřuje věrohodnost uživatele, ale jen totožnost síťové karty. Proces sdílené autentizační metody je popsán níže (obr. 2):



Obr. 2: Průběh autentizace sdíleným klíčem

1. Bezdrátový klient vyšle rámec 802.11 obsahující své identifikační údaje a požadavek pro sdílenou autentizaci.
2. Příjemce (typicky AP) odpoví vysláním rámce obsahující výzvu.
3. Bezdrátový klient zašifruje výzvu pomocí WEP a klíče, který je odvozen se sdíleného autentizačního klíče. Tu pak pošle, jakožto odpověď zpět k příjemci.
4. Příjemce dekóduje odpověď pomocí WEP a sdíleného klíče. Pak ji porovná s původně vyslanou výzvou z bodu 2, a pokud se shodují, vyšle rámec obsahující informaci o úspěšné autentizaci k síti. V opačném případě pošle rámec obsahující informaci o neúspěšném pokusu autentizace.

Dalším závažným problémem autentizace sdíleným klíčem se stává samotný, jednoduchý způsob takovéto autentizace. Při autentizaci se přenáší nešifrovaný text (výzva) s následně tím samým textem, ale zašifrovaným (odpověď). Útočník tak může odchytit zprávu o úspěšné autentizaci sdíleným klíčem a zjistit z ní sdílený autentizací klíč, který je ten samý, jako WEP šifrovací klíč a tím získat přístup do sítě. Pochopitelně, používání autentizace na základě sdíleného klíče nelze doporučit ani pro malé kanceláře nebo domácnosti.

2.1.1.3 Správa autentizačních klíčů

Standard 802.11 nedefinuje žádná pravidla správy a distribuce klíčů. Uživatel tak musí manuálně nastavovat klíče. Skutečnost, že je klíč sdílený, umožňuje ostatním uživatelům v síti odposlouchávat data přenášená jinými uživateli.

Z důvodu, že sdílený klíč musí být manuálně vložen do všech zařízení komunikujících v dané sítí, navíc, sdílený klíč je pro všechny zařízení stejný, stává se toto řešení zcela neergonomickým pro rozsáhlejší firemní infrastruktury. Kupříkladu, pokud je odcizen firemní notebook, tak aby útočník z něj neměl přístup do sítě firmy, musí být změněn sdílený WEP klíč na všech ostatních stanicích a přístupových bodech.

2.1.1.4 Konfigurace

Klíč je možno zadávat jako řetězec ASCII znaků, nebo jako jejich hexadecimální obdobu. Klíč o délce 64 bitů se zadává za pomoci 5 ASCII znaků nebo 10 hexadecimálních číslic (40 bitů pro klíč a 24 bitů pro inicializační vektor IV). Další varianta počítající se 128 bitovým klíčem obsahuje 13 ASCII znaků (26 hexadecimálních číslic) a 24 zbývajících bitů náleží inicializačnímu vektoru IV. Některá AP poskytují podporu i pro 152 bitový klíč. Jedná se však o nadstandardní doplněk.

Konkrétní příklad nastavení klíče v Linuxu:

- Nastavení klíče (128bit) pomocí ASCII znaků:
  `iwconfig` `wlan0` **`key s:`**`wephesloksiti`

- Natavení klíče (128bit) pomocí hexadecimálních číslic:
  `iwconfig` `wlan0` **`key`** `7765706865736c6f6b73697469`

- Následné zapnutí sdílené autentizace:
  `iwconfig` `wlan0` **`enc restricted`**

2.1.2 Šifrování a zajištění integrity datových přenosů

Nastavení bitu `Protected Frame` do hlavičky rámce 802.11 indikuje použití WEP šifrování v datovém přenosu. WEP používá dva druhy sdílených klíčů:

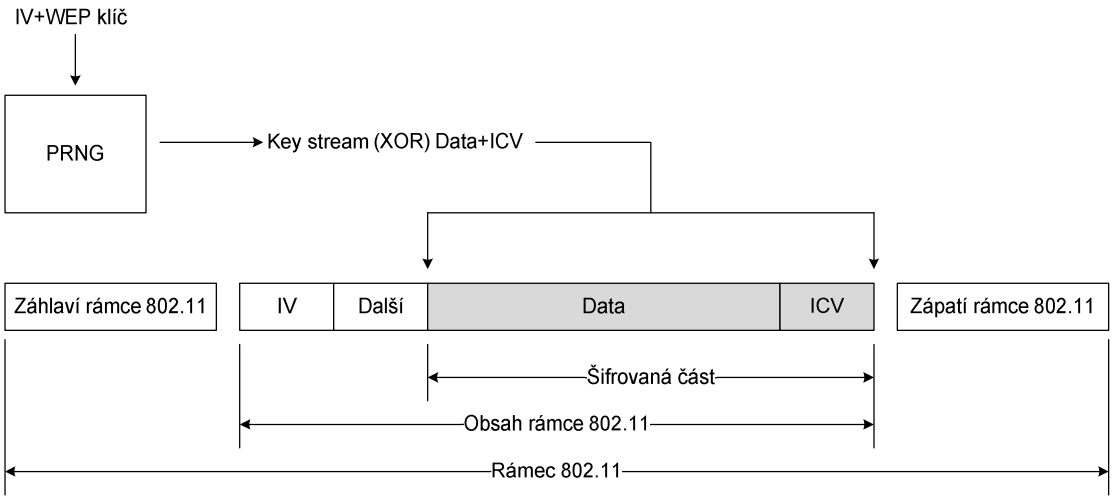
- Skupinový/globální klíč – tento klíč slouží na ochranu skupinového provozu od AP ke všem připojeným bezdrátovým klientům.
- Relační klíč – tento klíč slouží na ochranu jedinečně adresovaného provozu (unicast) mezi klientem a AP a současně na ochranu provozu skupinového a všeobecného (multicast a broadcast) od klienta směrem k AP.

Šifrování WEP využívá RC4 symetrickou proudovou šifru [1] se 40 resp. 104 bitovými šifrovacími klíči. Ačkoli 104 bitové klíče nejsou přímo specifikovány ve standardu 802.11, většina bezdrátových AP je přesto podporuje.

Některé implementace o sobě prohlašují, že podporují i 128 bitové WEP šifrování. Často se však jedná o klasický 104 bitový klíč v součtu s 24 bitovým IV vektorem. IV je sekvence 24 bitů v hlavičce každého rámce 802.11, a používá se při zašifrování i dešifrování přenášených dat, jak je ukázáno v následujících odstavcích. Problémem však zůstává to, že slabiny WEP se s delším klíčem nijak výrazně nemění [2].

2.1.2.1 Proces šifrování WEP

Šifrování rámce 802.11 prostřednictvím WEP (obr. 3):

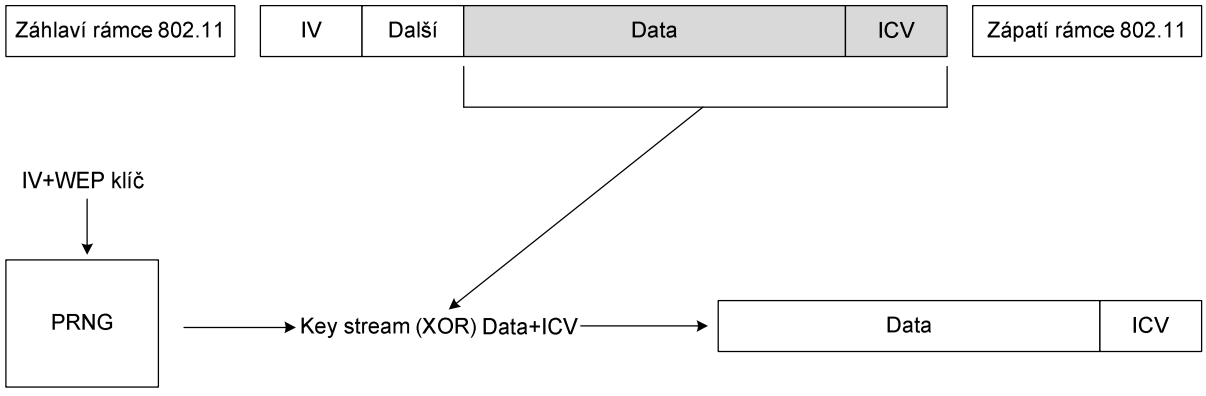


Obr. 3: Proces WEP šifrování

1. Z dat, která budou odeslána v rámci 802.11 je vypočítána 32 bitová hodnota ICV.
2. Hodnota ICV je připojená k datové části odesílaného rámce.
3. K WEP šifrovacímu klíči je připojena hodnota 24 bitového IV.
4. Výsledná kombinace (IV a WEP šifrovacího klíče) je využita pro vygenerování bitové sekvence pomocí pseudonáhodného generátoru (PRNG), která je stejně dlouhá jako původní kombinace IV a WEP šifrovacího klíče.
5. Na výsledné šifře – PRNG sekvenci bitů, známé taktéž jako Key stream se provede funkce XOR s hodnotou vstupních dat spolu s ICV.
6. IV se předřadí před zašifrovaná data a ICV a rámec se zapouzdří, když se přidá záhlaví rámce 802.11.

2.1.2.2 Proces dešifrování WEP

Dešifrování rámce prostřednictvím WEP (obr. 4):



Obr. 4: Proces dešifrování WEP

1. IV je získáno z nešifrované části příchozího rámce 802.11.
2. K IV je připojen WEP šifrovací klíč.

3. Tato kombinace (IV a WEP šifrovací klíč) je použita pro vstup do stejného PRNG k vygenerování sekvence bitů o délce dat a ICV. V tomto kroku se vygenerují stejná data, jako při původním šifrování.
4. Je provedena funkce XOR mezi vzniklou sekvencí bitů PRNG (Key stream) a zašifrovanými daty a ICV.
5. Nyní se vypočítá znovu hodnota ICV a pokud se nová hodnota ICV shoduje s došlou a dešifrovanou ICV hodnotou, lze data považovat za integritně korektní (čili, že v průběhu přenosu od klienta nebyly modifikovány ani jinak poškozeny). Pokud ICV nesouhlasí, rámec je zahozen.

Zatímco WEP klíč zůstává stejný, IV se dynamicky mění. Není však standardizováno, jak často se má IV měnit. Ideální stav je, pokud se mění v každém vyslaném rámci a při inicializaci síťové karty nezačíná od nuly a dál se s každým paketem nezvyšuje o jedno [3].

2.1.2.3 Zajištění integrity v datových rámcích 802.11

WEP nabízí kromě šifrování i zajištění integrity přenášených dat. Provádí kontrolní součet datové části rámce pomocí funkce cyklického kontrolního součtu CRC-32 [4], jehož výsledkem je ICV (Integrity Check Value). Ten se připojuje k rámci za jeho datovou část. ICV má velikost 4 bajtů. Z následně přijatého rámce se znovu sestaví kontrolní součet CRC-32, a pokud souhlasí se součtem doručeným v posledním rámci, data jsou neporušená.

2.1.3 Další možnosti zabezpečení sítí 802.11

Jako doplněk šifrování WEP bývají k zabezpečení sítě založené na standardu 802.11 používány tyto techniky:

- Skrytí SSID
- Filtrace MAC adres

2.1.3.1 Skrytí SSID

Většina bezdrátových AP může být konfigurována tak aby nevysílala SSID, což je označení pro textový identifikátor bezdrátové sítě. V takovém případě jsou tyto sítě známé jako skryté. Cílem této funkce je zamezení detekce takové sítě neautorizovanými uživateli. Přesto však, takto skrytou síť mohou útočníci za jistých okolností rozpoznat, což popíšu dále.

2.1.3.1.1 Konfigurace

Na softwarovém AP v linuxovém prostředí je možno vypnout vysílání SSID dle zvoleného zařízení a příslušného ovladače. Například, pokud je používán ovladač MadWi-Fi spolu s některým z podporovaných Atheros čipsetů, je možno vypnout vysílání SSID příkazem:

```
iwpriv wlan0 hide_ssid 1
```

Při použití ovladače HostAP pak příkazem:

```
iwpriv wlan0 enh_sec 1
```

2.1.3.1.2 Slabiny a možnosti útoků

Klienti sítě, kdy je vypnuto vysílání SSID, musí dané SSID znát. Nicméně, když se klient připojuje k AP, musí SSID vyslat v nezašifrované podobě v asociačním rámci. Pro útočníka tak platí, že si může SSID odposlechnout právě tehdy, když se nějaký klient připojuje k AP. Další skutečnost oslabující smysl skrytí SSID z hlediska bezpečnosti sítě je, že útočníkovi stačí odposlouchávat rámce vysíláne nikoli klientem, ale samotným AP. Klient před připojením totiž vysílá tzv. Probe rámce, kterými vyshledává daný přístupový bod pomocí SSID, které je v Probe rámci uloženo, AP následně klientovi odpovídá, opět se svým SSID, a právě zde se vyskytuje příležitost, jak zachytit SSID ze strany AP.

Vhodnou programovou implementací v linuxovém prostředí pro útočníka je program Kismet, který je schopen zjistit SSID ze zachycených rámců.

Po spuštění zobrazí Kismet SSID přístupových bodů v okolí, které jsou veřejné resp. těch, které vysílají Beacon rámce obsahující SSID. U skrytých sítí se nejprve ve sloupci Name zobrazuje hodnota `<no ssid>`, dokud Kismet nepřijme asociační rámec dané stanice. Ve výpisu se pak objeví zpráva:

```
Found SSID "PrivateNet" for cloaked network BSSID
00:AA:BB:CC:DD:EE
```

Nově zjištěné SSID se pak zobrazí ve sloupci se jménem sítě místo původního `<no ssid>`.

2.1.3.2 Filtrace MAC adres

Většina bezdrátových AP umožňují funkci filtrace MAC adres. Jelikož je, nebo lépe řečeno, měla by být MAC adresa jedinečná pro každou síťovou kartu, je možné sestavit seznam MAC adres, které mají povolený přístup do sítě. Klient s neregistrovanou MAC adresou se pak nemůže připojit.

2.1.3.2.1 Konfigurace

V Linuxu je možnost sestavit seznam povolených MAC adres příkazem iwpriv pro dané síťové rozhraní. Nejprve je však třeba nastavit samotnou funkci filtrace MAC adres:

```
iwpriv wlan0 maccmd 1
```

Nyní již můžeme nastavit konkrétní požadovanou MAC adresu, kterou tímto registrujeme, jako povolenou pro přístup do sítě:

```
iwpriv wlan0 addmac 00:1D:0F:D3:5E:70
```

2.1.3.2.2 Slabiny a možnosti útoků

MAC adresu síťové karty je velice snadné změnit. Aby síťová karta mohla fungovat jako bridge, musí umět odesílat pakety s libovolnou MAC adresou. Pokud tedy zjistíme, jakou MAC adresu máme nastavit, která je už v síti registrovaná, můžeme tím získat přístup do sítě samotné.

K tomuto jsem využil tcpdump, který k následně potřebným úkonům stačí. Nejprve je potřeba nastavit síťovou kartu do módu monitor, aby zachytávala všechny pakety:

```
iwconfig wlan0 mode monitor
```

Dále pak je potřeba nastavit kanál, na kterém bezdrátové AP vysílá, v tomto případě to byl kanál 6:

```
iwconfig wlan0 channel 6
```

Nyní pomocí programu tcpdump můžeme odchytit provoz v síti:

```
tcpdump -nei wlan0 ip
```

Pro nás, důležitá část výpisu vypadá takto:

```
DA:00:1D:0F:D3:5E:70 BSSID: 00:AA:BB:CC:DD:EE
SA:00:AA:BB:CC:DD:EE ethertype Ipv4 (0x0800): 213.235.157.34.80
> 192.168.1.100: TCP
```

Na výpisu je možné si všimnout, že SA (zdrojová adresa) je shodná s BSSID (MAC adresa přístupového bodu). Z toho vyplývá, že paket byl vyslán z AP. V tomto momentě stačí vzít cílovou IP `(192.168.1.100)` a MAC `(00:1D:0F:D3:5E:70)` adresu změnit si tyto hodnoty u naší síťové karty k obrazu svému. V Linuxu lze změnit MAC adresa příkazem:

```
ifconfig wlan0 hw ether 00:1D:0F:D3:5E:70
```

Tento typ zabezpečení je velice slabý, ačkoli pro uživatele – klienta, velice komfortní, pokud nepřistupuje do sítě s novým zařízením s rozdílnou MAC adresou. Ta se totiž musí znovu nastavit ve filtru MAC adres pro dané AP. Každopádně filtraci MAC adres lze doporučit z hlediska bezpečnosti maximálně jako doplněk k sofistikovanějším metodám zabezpečení.

2.1.4 Shrnutí bezpečnostních rizik standardu IEEE 802.11

Hlavním neduhem v zabezpečení pomocí WEP je skutečnost, že odvození a distribuce WEP šifrovacích klíčů není nijak standardizována. Klíče WEP musí být distribuovány jinou cestou, než pomocí protokolu 802.11. Prakticky to znamená, že WEP klíč je manuálně nakonfigurován jak na straně klienta, tak i na straně bezdrátového AP. Tímto způsobem distribuované klíče však nelze považovat za bezpečné a ani vhodné pro firemní sektor.

Navíc, není specifikovaný mechanismus povinné změny WEP šifrovacího klíče. Všechna bezdrátová AP a klienti v dané síti používají obvykle jeden WEP klíč po dlouhou dobu. V síti s více připojenými klienty, a tak s větším očekávaným datovým tokem, je pro útočníka velice snadné rozluštit WEP klíč pomocí kryptoanalytických metod a získat tak přístup do sítě.

Hlavními bezpečnostními riziky standardu 802.11 jsou tedy tato:

- Nemožnost detekce falešných bezdrátových AP.
- Autentizace probíhá na úrovni jednotlivého zařízení, nikoli na úrovni uživatelů.
- Žádný centralizovaný mechanismus pro autentizaci, autorizaci a účtování.
- Neexistuje zde podpora pro rozšířenou autentizaci například pomocí jednorázového hesla, čipové karty nebo certifikátu.
- Chybí podpora managementu klíčů, například změna klíčů v pevně stanovených intervalech nebo při opětovné autentizaci.

Tyto problémy původního standardu 802.11 však řeší standard 802.1x.

2.2 Autentizace pomocí standardu 802.1x

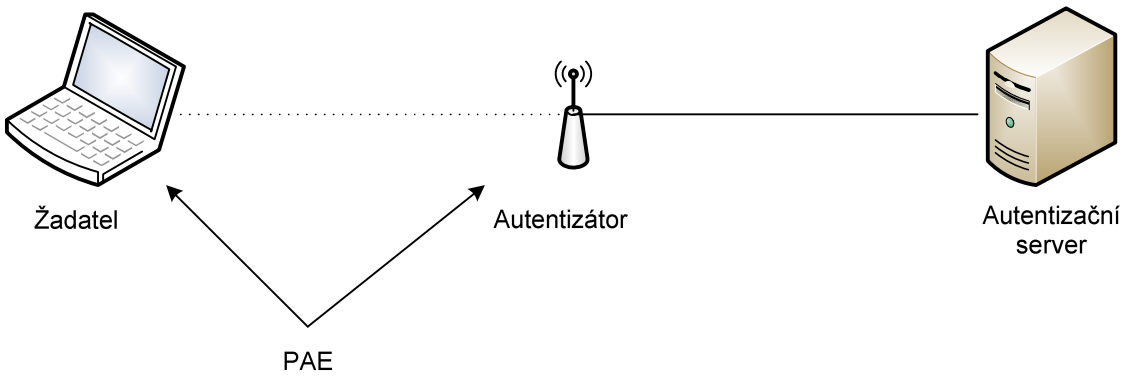
Standard IEEE 802.1x definuje řízení přístupu k síti na základě otevřených portů pro zabezpečení sítí LAN. Tento standard má za cíl blokovat přístup neoprávněných uživatelů k segmentu lokální sítě. Autentizace je vzájemná a probíhá mezi uživatelem a autentizacím serverem (RADIUS). Využívá se zde dynamického generování klíčů, na uživatele a pro relaci. Dynamické klíče jsou známy pouze dané stanici, mají omezenou životnost a používají se k šifrování rámců na daném portu, dokud se stanice neodhlásí nebo neodpojí. Standard 802.1x je založený na protokolu EAP (Extensible Authentication Protocol), který podporuje více autentizačních mechanismů. Ačkoli se jedná o standard původně vytvořený pro sítě LAN, byl přizpůsoben i pro použití v bezdrátových sítích založených na standardu 802.11.

2.2.1 Prvky 802.1x

Autentizace pomocí 802.1x se účastní následující subjekty:

- PAE (Port Access Entity) – jednotka přístupu k portu
- Autentizátor
- Žadatel
- Autentizační server

Schéma (obr. 5) zobrazuje tyto komponenty v bezdrátové síti:



Obr. 5: Složky autentizace 802.1x

PAE (Port Access Entity) je protokolovou jednotkou, přičleněnou k portu, logickou jednotkou podporující standard 802.1x. Může na sebe vzít roli autentizátora, žadatele nebo obou.

Autentizátor je v bezdrátové síti přístupový bod umožňující samotnou autentizaci žadatele, přeposílá komunikaci mezi žadatelem a autentizacím serverem k ověření přístupu do sítě.

Žadatel je klient, který se chce připojit do sítě a poskytuje své identifikační údaje pro ověření autentizacím serverem.

Autentizační server (nejčastěji RADIUS) udržuje databázi ověřených uživatelů a při pokusu o přihlášení uživatele do sítě provádí jeho ověření.

2.2.2 Rámec pro autentizaci: EAP

EAP (Extensible Authentication Protocol) je rámcem pro autentizaci v 802.1x. Konkrétní autentizační metoda pak tento rámec využívá. Komunikace probíhá prostřednictvím zpráv, které jsou baleny přímo do linkových rámců, ne do IP paketů. EAP podporuje přes 30 autentizačních metod. Ne všechny jsou však kompatibilní se všemi klienty v síti a s autentizačním serverem zároveň. Je tedy potřeba vybrat takové autentizační metody, kdy je pravděpodobnost nekonfliktnosti z hlediska kompatibility co největší.

Aby útočník nemohl vytvořit falešný přístupový bod, čímž by sice nezískal přímý přístup do sítě, ale mohl by odposlouchávat komunikaci klientů, je potřeba využít autentizace vzájemné, to znamená, že žadatele musí autentizovat vůči autentizačnímu serveru, ale i samotný autentizační server se musí jednoznačně autentizovat vůči žadateli. Autentizace má tak tedy obvykle dvě fáze. Nejprve klient zkontroluje certifikát serveru a vytvoří šifrovaný tunel pomocí protokolu TLS. Poté, v druhé fázi, proběhne samotná autentizace klienta vůči serveru. Na tomto principu fungují metody EAP-PEAP a EAP-TTLS.

2.2.3 Shrnutí řešených problémů 802.11 pomocí 802.1x

Standard 802.1x naštěstí řeší spoustu bezpečnostních rizik původního 802.11. Jsou to tyto (původní neduhy IEEE 802.11 jsou nadepsány tučně):

- **Nemožnost detekce falešných bezdrátových AP**
  Nejlepším řešením na ochranu proti falešným bezdrátovým AP je podpora a implementace vzájemného autentizačního protokolu, jakými jsou EAP-TLS nebo PEAP-MS-CHAP v2. Pomocí těchto protokolů si žadatel dokáže ověřit dané AP, na které se připojuje, a to na základě prověření certifikátu RADIUS serveru.
- **Autentizace probíhá na úrovni jednotlivého zařízení, nikoli na úrovni uživatelů.**
  IEEE 802.1x řeší tento problém, neboť zde se k přístupu do sítě ověřuje samotný uživatel na základě autentizačního rámce EAP, nikoli pouze zařízení, které může být odcizeno, využito jiným neoprávněným uživatelem a podobně.
- **Žádný centralizovaný mechanismus pro autentizaci, autorizaci a účtování.**
  Použitím RADIUS serveru ve spojení s IEEE 802.1x odpadá tato nepraktická složka původního standardu IEEE 802.11. RADIUS se tak může stát komplexním nástrojem pro autentizaci, autorizaci a účtování.
- **Neexistuje zde podpora pro rozšířenou autentizaci například pomocí jednorázového hesla, čipové karty nebo certifikátu.**
  IEEE 802.1x používáním rámce pro autentizaci EAP řeší tento problém, neboť EAP je obecně navržen pro jakoukoli autentizační metodu.
- **Chybí podpora managementu klíčů, například změna klíčů v pevně stanovených intervalech nebo při opětovné autentizaci.**
  Použitím standardu IEEE802.1x a jedné z autentizačních metod, EAP-TLS nebo PEAP-MS-CHAP v2, jak jsem ukázal, jsou dynamicky generovány klíče pro každou relaci – klíče se mění po pevně stanovených intervalech a při každé opětovné autentizaci.

Přesto, že IEEE 802.1x řeší spoustu bezpečnostních slabin původního standardu IEEE 802.11, stále neřeší kryptografické slabiny samotného WEP:

- **IV je příliš krátký**
  WEP používá IV spolu s WEP šifrovacím klíčem jako vstup do RC4 PRNG, který produkuje proudovou šifru pro zašifrování obsahu rámce standardu 802.11. S pouhým 24 bitovým IV je pro útočníka snadné zachytit dostatečný počet WEP rámců se stejnou hodnotou IV, což činí rozšifrování snadnějším.
- **Slabé zajištění integrity dat**
  Integritu dat ve WEP zajišťuje kontrolní součet CRC-32, který je vypočítán na základě posílaných dat v daném rámci a následně do něj připojen. Je poměrně jednoduché zaměnit hodnotu CRC-32 v souladu s pozměněnou hodnotou dat v rámci, aniž by příjemce byl scjopen toto rozpoznat.
- **Použití hlavního klíče místo odvozeného**
  WEP klíč, ať už manuálně nakonfigurován nebo odvozen pomocí autentizace 802.1x lze označit za hlavní klíč, je používán k šifrování dat, což je méně bezpečné než použití klíče odvozeného od hlavního klíče pro tyto účely.
- **Žádná obnova klíčů**
  WEP nenabízí žádnou funkci pro obnovu šifrovacích klíčů.
- **Neexistuje obrana proti útokům typu replay**
  WEP neposkytuje žádnou ochranu před útoky typu replay. Tento útok spočívá v odposlouchávání části komunikace mezi dvěma autentizujícími se stranami a následném použití odchycených dat k autentizaci útočníka.

Odstranit tyto neduhy se snaží postupně WPA a pak doplněk 802.11i, který popíšu v následující kapitole.

2.3 WPA jako přechodový můstek k 802.11i

Bezpečnostní mechanismus WPA (Wi-Fi Protected Access) odstraňuje všechny známé chyby svého předchůdce WEP. WPA používá mechanismy, které v době jeho uvedení (konec roku 2002) byly ve vývoji pro nadcházející bezpečnostní doplňek 802.11i. Jednalo se tedy o dočasné řešení vzniklé situace, kdy se WEP prokázal být nedostatečným bezpečnostním mechanismem pro ochranu bezdrátových přenosů v IEEE 802.11. Do WPA byly implementovány však jen ty vylepšení, které nevyžadovaly fyzický upgrade přístupových bodů. U většiny AP tak stačilo nahrát nový firmware, který měl v sobě již zabudovanou podporu pro WPA. WPA je tedy podmnožinou prvků 802.11i.

WPA zahrnuje vylepšení následujících aspektů bezpečné bezdrátové komunikace:

- Autentizace
- Šifrování přenášených dat
- Datová integrita

2.3.1 Autentizace

Zatímco v původním standardu 802.11 je autentizace pomocí 802.1x volitelná. S WPA je tato autentizace podmíněná. Autentizace s WPA je kombinací systému otevřené autentizace a autentizace pomocí 802.1x.

Řešením pro malé nebo domácí kanceláře popřípadě jiné malé sítě je použití pro autentizaci režimu přednastaveného klíče, tzv. PSK. K ověření žadatele se používá sdílený klíč, který musí znát každé zařízení, které se chce připojit. O výsledku autentizace rozhoduje AP, na základě klíče poskytnutého klientem. Pokud klíč poskytnutý klientem souhlasí s klíčem uloženým v AP, je klient úspěšně autentizován.

Pro větší sítě, jako jsou třeba podniková prostředí, předpokládá WPA využití centralizovaného serveru zodpovědného za distribuci klíčů (typicky RADIUS). Každý uživatel má jiné přihlašovací údaje. O povolení přístupu k sítí pak nerozhoduje AP, ale právě autentizační server. Oproti PSK módu se jedná o robustnější zabezpečení. Jako rámec pro autentizace se zde využívá EAP.

2.3.2 Šifrování přenášených dat

WPA podporuje dvě metody šifrování přenášených dat:

- TKIP
- AES

TKIP (Temporal Key Integrity Protocol) využívá stále šifrovacího algoritmu RC4. Klíč má taktéž standardní délku 128 bitů. Avšak hlavním vylepšením oproti WEPu je dynamické generování klíčů a delší IV (48 oproti původním 24). TKIP nahrazuje WEP díky novému šifrovacímu algoritmu, který je silnější, než WEP. Důležité je, že tento algoritmus lze provádět i na starších zařízeních, původně podporujících pouze WEP, po nezbytném upgradu firmware.

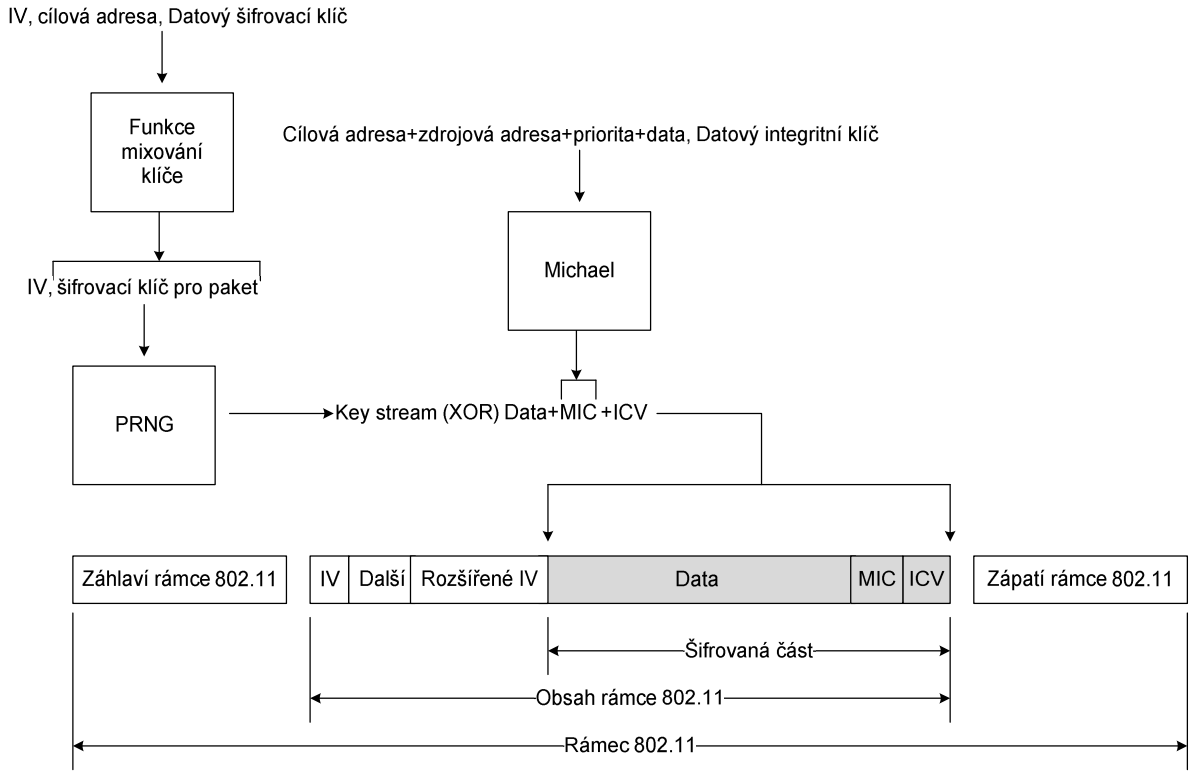
WPA umožňuje použití i AES (Advanced Encryption standard), jako volitelnou náhradu šifrování WEP. U starších zařízení však tuto podporu nelze dodat softwarově pomocí nového firmware. Podpora AES je proto nepovinná a záleží na každém výrobci, zda ji implementuje nebo ne.

2.3.2.1 Proces šifrování WPA

WPA potřebuje tyto hodnoty pro zašifrování a datovou integritu datového rámce:

- IV, který začíná nulou a tato hodnota se inkrementuje každý následující rámec.
- Datový šifrovací klíč (pro unicastový provoz) nebo skupinový šifrovací klíč (pro multicastový provoz).
- Zdrojovou a cílovou adresu rámce.
- Hodnotu priority, která je rezervována pro užití v budoucnosti.
- Datový integritní klíč (pro unicastový provoz) nebo skupinový integritní klíč (pro multicastový provoz).

Dále uvádím schéma (obr. 6) a popis WPA šifrovacího procesu pro unicastový datový rámec.

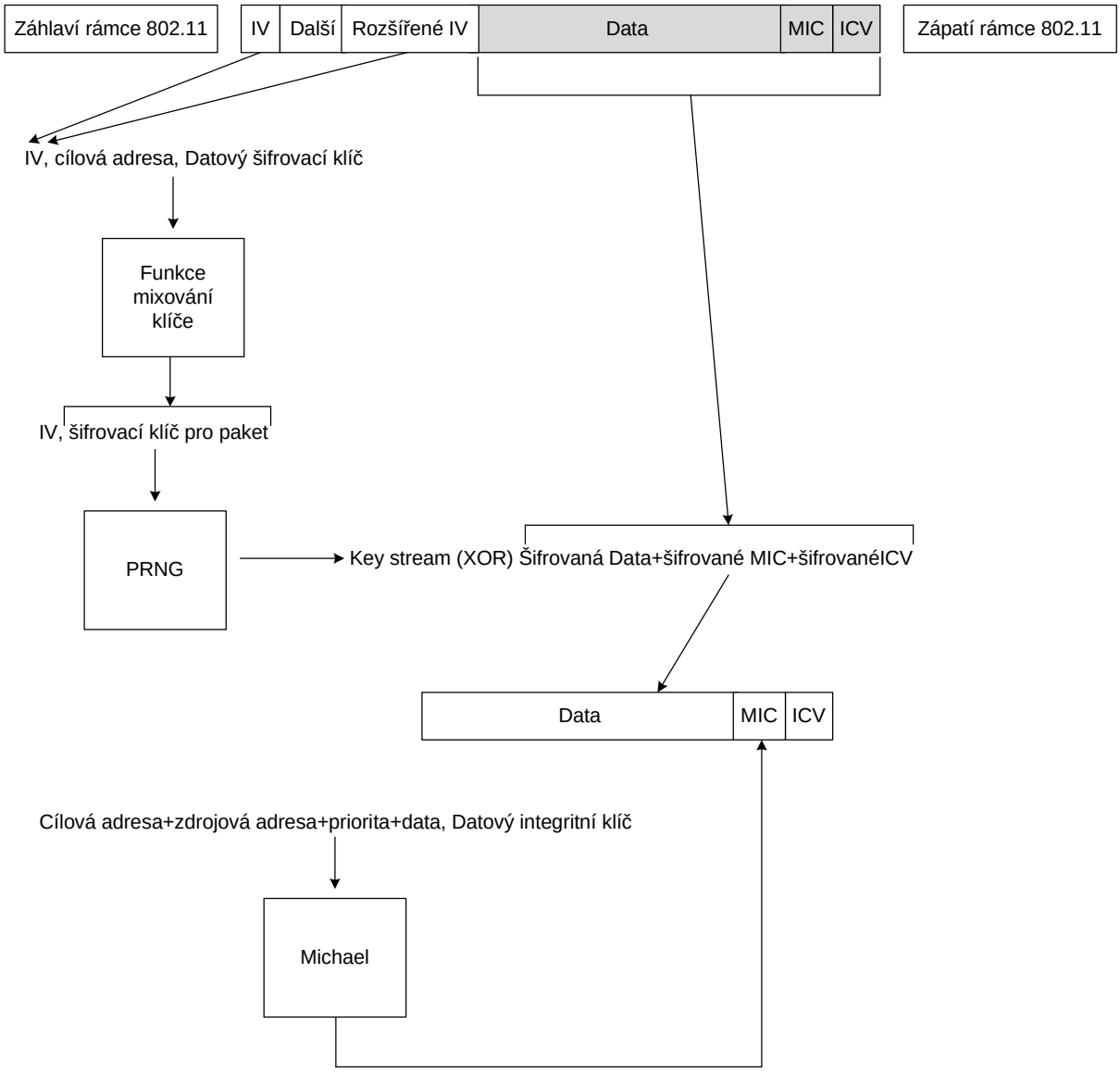


Obr. 6: Proces šifrování WPA

1. IV, cílová adresa a datový šifrovací klíč jsou zpracovány WPA funkcí mixování klíče, která vypočítá šifrovací klíč pro paket.
2. Cílová adresa, zdrojová adresa, priorita, data a datový integritní klíč jsou vloženy do algoritmu datové integrity Michael a výstupem je MIC (Message Integrity Check).
3. Je vypočítána hodnota ICV pomocí kontrolního součtu CRC-32.
4. IV a šifrovací klíč pro paket jsou vloženy jako vstup do RC4 PRNG funkce pro vyprodukování proudové šifry o velikosti dat, MIC a ICV dohromady.
5. Na výsledné šifře – PRNG sekvenci bitů, známé taktéž jako Key stream se provede funkce XOR s hodnotou vstupních dat spolu s MIC a ICV.
6. IV se přidá do obsahu rámce 802.11 jako IV a Rozšířené IV a nakonec se rámec zapouzdří záhlavím a zápatím rámce 802.11.

2.3.2.2 Proces dešifrování WPA

Na dalším schématu (obr. 7) je zobrazen proces a dále pak popis WPA dešifrování pro unicastový datový rámec:



Obr. 7: WPA – proces dešifrování rámce

1. Hodnota IV je extrahována z polí IV a Rozšířené IV z datového rámce 802.11. Poté je IV spolu s cílovou adresou a datovým šifrovacím klíčem vloženy jako vstup do funkce WPA mixování klíčů. Výstupem je šifrovací klíč pro paket.
2. IV a šifrovací klíč pro paket jsou vloženy jako vstup do RC4 PRNG funkce, jejímž výstupem je proudová šifra stejné velikosti jako zašifrovaná data spolu s MIC a ICV.
3. Je provedena funkce XOR mezi vzniklou proudovou šifrou (Key stream) a zašifrovanými daty, spolu s MIC a ICV.
4. ICV je vypočítána a porovnána s hodnotou dešifrované hodnoty ICV. Pokud data z ICV nejsou stejná, rámec je zahozen.

5. Cílová a zdrojová adresa, data a datový integritní klíč slouží jako vstup pro zpracování integritního algoritmu Michael. Výstupem je MIC.
6. Vypočítaná hodnota MIC je porovnána s hodnotou došlou v datovém rámci, následně dešifrovanou. Pokud se shodují, mohou být data zpracována vyššími síťovými vrstvami.

2.3.3 Zajištění integrity v datových rámcích

Kontrola integrity datového rámce se provádí pomocí MIC (Message Integrity Check), který se připojuje ke zprávě a získává se z dat a adres zprávy prostřednictvím funkce přezdívané Michael. Kontrolní součet MIC nahrazuje jednoduchý a nebezpečný vektor ICV používaný u WEP. MIC má na rozdíl od ICV dvojnásobnou délku a pro jeho vytvoření se používá jednocestná funkce nad některými poli záhlaví a daty rámce (viz obr. 6). Je odolný vůči útokům, které byly úspěšné u ICV, jako jsou záměny bitů nebo falšování záhlaví. Neodolá ovšem některým útokům typu DoS. Datový rámec však stále obsahuje i hodnotu ICV.

2.4 802.11i (WPA2)

Doplněk ke standardu s názvem IEEE 802.11i formálně nahrazuje WEP a další bezpečnostní zabezpečení původního standardu IEEEE 802.11.

Wi-Fi Protected Access 2 (WPA2) je certifikace produktu, kterou lze získat prostřednictvím sdružení Wi-Fi Alliance. Označení WPA2 potvrzuje, že bezdrátové vybavení je kompatibilní se standardem IEEE 802.11i. Produktová certifikace WPA2 formálně nahrazuje označení Wired Equivalent Privacy (WEP) a další bezpečnostní prvky původního standardu IEEE 802.11. Cílem certifikace WPA2 je podpora dalších povinných funkcí zabezpečení standardu IEEE 802.11i, které nejsou ještě zahrnuté do produktů, které podporují standard WPA.

2.4.1 Autentizace

Pro WPA2 Enterprise je vyžadována autentizace ve dvou fázích. První je otevřená systémová autentizace a druhá využívá 802.1x a autentizačního rámce EAP. Pro síťové infrastruktury bez RADIUS serveru, jako jsou malé kanceláře nebo domácnosti, WPA2 Personal podporuje použití předsdíleného klíče (PSK).

2.4.2 Management klíčů

WPA i WPA2 využívá stejného schématu při správě klíčů. Vytváření klíčů tedy probíhá v 802.11i dynamicky. Na vrcholu klíčové hierarchie serverových klíčů je PMK (pairwise master key). Za jeho vytvoření zodpovídá autentizační protokol použitý v průběhu autentizační fáze 802.1x. Protokoly standardu 802.1x vygenerují dočasný klíč a z něj autentizační server a klientský software žadatele vygenerují pár identických klíčů PMK. Server i stanice mají stejný klíč, nicméně je ještě nutno poskytnout kopii PMK pro AP. Autentizační klíč se zkopíruje z autentizačního serveru k autentizátorovi (AP) žadatele. Nyní se pomocí PMK vygenerují dočasné WPA2 klíče. Protože podobně jako WPA, tak i WPA2 používá několik párových klíčů pro unicastové rámce a zprávy EAPOL, k ochraně navazování komunikace. Klíče jsou pak tyto:

- Datový šifrovací klíč – 128 bitový klíč použitý k šifrování unicastových rámců.
- Datový integritní klíč – 128 bitový klíč použitý pro výpočet hodnoty MIC unicastových rámců.
- EAPOL šifrovací klíč – 128 bitový klíč použitý pro šifrování EAPOL zpráv.

- EAPOL integritní klíč – 128 bitový klíč sloužící k výpočtu hodnoty MIC v EAPOL zprávách.

2.4.3 Šifrování a integrita datových přenosů

CCMP je protokol zaručující silnější šifrování. CCMP používá 128 bitový klíč a na rozdíl od WEP, používá dynamické generování klíčů. CCMP zajišťuje jak šifrování, tak i integritu datových rámců, ale i například číslování paketů, které zabraňuje útokům typu replay. Pro šifrování přenášených dat se používá AES (Advance Encryption Standard), který využívá Counter Mode – Cipher Block Chaining (CBC) –Message Authentication Code (MAC) Protocol (CCMP). AES Counter Mode je bloková šifra která zašifruje 128 bitové bloky dat pomocí 128 bitového klíče. Algoritmus CBC-MAC produkuje MIC, který slouží pro zachování integrity datového rámce. Do WPA2 rámce je taktéž vložena hodnota pořadí rámce, jako ochrana proti replay útokům. Šifrování AES vyhovuje i vládním účelům. Díky celkovému návrhu AES není potřeba generovat klíče pro každý zaslaný rámec. CCMP proto používá relační klíč pro šifrování dat a generování kontrolního součtu.

Zatímco při použití původního standardu IEEE 802.11 stačilo útočníkovi odposlechnout dostatečný objem zpráv, aby mohl zlomit klíč WEP, a jedinou obranou bylo manuálně klíče často měnit, mění 802.11i klíče automaticky [8].

IEEE 802.11i tak nabízí řešení známých nedostatků původního WEP:

- **IV je příliš krátký**
  V AES CCMP je IV nahrazen paketovým pořadovým číslem, jehož délka je 48 bitů.
- **Slabé zajištění integrity dat**
  Algoritmus CRC-32 je nahrazen algoritmem AES CBC-MAC, který je navržen k zachování silné datové integrity. Výstupem algoritmu CBC-MAC je 128 bitová hodnota, přičemž WPA2 využije výsledných 64 bitů s vyšší váhou jako MIC. WPA2 šifruje MIC pomocí AES Counter Mode.
- **Použití hlavního klíče místo odvozeného**
  Podobně jako u WPA a u něj využívaného TKIP, AES CCMP používá sadu dočasných klíčů, které jsou odvozeny z hlavního klíče a dalších hodnot. Hlavní klíč je odvozen z EAP-TLS nebo PEAP autentizačního procesu 802.1x.
- **Žádná obnova klíčů**
  AES CCMP obnovuje klíče automaticky pro odvození nových dočasných klíčů.
- **Neexistuje obrana proti útokům typu replay**
  AES CCMP používá hodnotu čísla paketu jako ochranu před útoky typu replay.

2.5 Možnosti zabezpečených bezdrátových přenosů v typických síťových topologiích

V předešlých kapitolách jsem popsal, zhodnotil a na ukázkových konfiguracích ukázal jednotlivé možností zabezpečení bezdrátových sítí standardu IEEE 802.11. Nyní na příkladech síťových topologií ukážu, jakou bych volil konfiguraci v jejich jednotlivých případech.

2.5.1 Poskytovatel internetu (ISP)

Hlavním nedostatkem nasazení Wi-Fi sítí pro poskytovatele internetu do oblastí poslední míle je fakt, že k tomuto účelu nebyl původně standard IEEE 802.11 a jeho deriváty navržen. Nicméně poměrně nízké náklady na zprovoznění takové sítě způsobily její rozmach i v tomto ohledu. Pokud bych uvažoval poskytovatele, který bezdrátově připojuje k Internetu klienty v okolí svých přístupových bodů, je nutno zajistit a zvážit několik řešení z hlediska bezpečnosti. V ideálním případě je nutno zajistit, aby se do sítě nemohl připojit jak někdo cizí, stejně tak jako bývalý zákazník, který již není registrován jako uživatel dané sítě.

Na první pohled se z hlediska bezpečnosti jeví jako dobré řešení zabezpečit síť pomocí WPA2-EAP s autentizací PEAP/MSCHAPv2, jak uvádím příklady konfigurace v kapitole 4.3. Pro poskytovatele internetu to však znamená dost složitou režii. Jako cenově velice schopné řešení se mi jeví použit na straně žadatele zařízení, které slouží jako switch, Wi-Fi AP a kvalitní router zároveň. Další podmínkou kvůli zabezpečení je, možnost nahrát na něj místo originálního firmware Linuxovou distribuci OpenWRT [9]. To poskytuje možnost mimo jiné instalaci programu wpa_supplicant a tak zajistit bezpečný přístup do bezdrátové sítě. Seznam podporovaných zařízení pro nahrání OpenWRT je uveden na domácí stránce projektu. Snad bych jen zmínil, že docela široké podpoře se těší zařízení Linksys, například typ Linksys WRT54GL za méně než 2000 Kč, s kterým jsem měl možnost pracovat. Je to sice trochu komplikovaná cesta, jak zabezpečit síť lokálního ISP, nicméně pokud to poskytovatel myslí s bezpečností vážně, mnoho možností u klasického Wi-Fi připojení nemá.

Byl jsem však překvapen, že mnoho poskytovatelů v mém okolí zabezpečuje svou síť stále pomocí WEP spolu s filtrací MAC adres. Poskytovatele k tomu mohou vést pravděpodobně starší nebo extrémně levná zařízení na straně zákazníků. Výměna hardware na straně zákazníků by byla nejspíše dosti nákladná a tak poskytovatel musí zvážit rizika a výhody, která z tohoto nedostatečného zabezpečení sítě nastávají. Výhodou je sice jednoduchost takovou síť spravovat, útočník se však může do sítě připojit a snižovat tak využitelnou kapacitu sítě pro ostatní původně oprávněné uživatele této sítě.

2.5.2 Firemní síť

Bezdrátové sítě hrají v dnešní době velice důležitou roli, hlavně s rozmachem používání notebooků, které mají obvykle integrovanou síťovou kartu pro bezdrátový přístup do potřebné sítě založené na standardech IEEE 802.11(a/)b/g. Dalšími důvody pro nasazení bezdrátového připojení ve firmě jsou důvody ekonomické, kdy tahání kabeláží může být dosti náročným finančním úkonem, navíc oproti bezdrátovým sítím, pro koncové uživatele (žadatele) i nepohodlným.

Firemní bezdrátová síť by měla používat zabezpečení WPA-EAP s autentizací PEAP/MSCHAPv2 nebo EAP-TLS. Heslo uživatele by mělo být v případě autentizace PEAP/MSCHAPv2 silné, neprolomitelné slovníkovým útokem. Stejně tak i heslo mezi RADIUS serverem a AP by mělo mít stejné vlastnosti.

Pokud firma využívá přístup uživatelů do firemní sítě prostřednictvím VPN [10], je možné umístit bezdrátovou síť přes firewall a dovolit z ní přístup jen na VPN server. Bezdrátovou síť pak nemusíme zabezpečovat, přístup bude zabezpečovat VPN stejně jako přístup přes Internet.

Při odcizení síťového zařízení nebo notebooku je nutno co nejrychleji toto nahlásit, aby se zabránilo přístupu do sítě neoprávněnému uživateli pomocí přístupových informací uložených v paměti operačního systému.

2.5.3 Domácí síť nebo malá firma

Zabezpečení domácích sítí nebo malých firem, přibližně do deseti zaměstnanců využívající síťové služby podniku, naštěstí není tak komplikované, jako zabezpečení firem nebo sítí poskytovatelů internetu. Je však s podivem, že v době, kdy i nejlevnější AP/routery nabízejí ochranu přenášených dat prostřednictvím WPA2, mnoho neznalých uživatelů používá v tom lepším případě stále WEP. V tom horším případě nezabezpečují svou síť vůbec.

V současnosti je tak nejlepší volbou zapnout šifrování WPA2-PSK, pokud s touto metodou nemá problém operační systém uživatele. Dále lze pro doplnění bezpečnosti vypnout vysílání SSID a nakonfigurovat na AP filtraci MAC adres. Silné heslo schopné odolat slovníkovým útokům by mělo být samozřejmostí.

2.5.4 Shrnutí možných zabezpečení pro různé síťové topologie

Následující tabulka (tab. 1) shrnuje, které možnosti zabezpečení jsou vhodné pro daný typ sítě.

	Poskytovatel Internetu	**Firemní síť**	**Domácí síť/malá firma**
WEP	Nevyhovující	Nevyhovující	Nevyhovující
WEP+802.1x	Použitelné	Použitelné	Zbytečné
WPA-PSK	Nevyhovující	Nevyhovující	Vhodné
WPA-EAP	Vhodné	Vhodné	Zbytečné
WPA2-PSK	Nevyhovující	Nevyhovující	Vhodné
WPA2-EAP	Vhodné	Vhodné	Zbytečné
Doplňky síťového zabezpečení			
Filtrace MAC	Zbytečné	Zbytečné	Zbytečné
Skrytí SSID	Nevhodné	Zbytečné	Vhodné

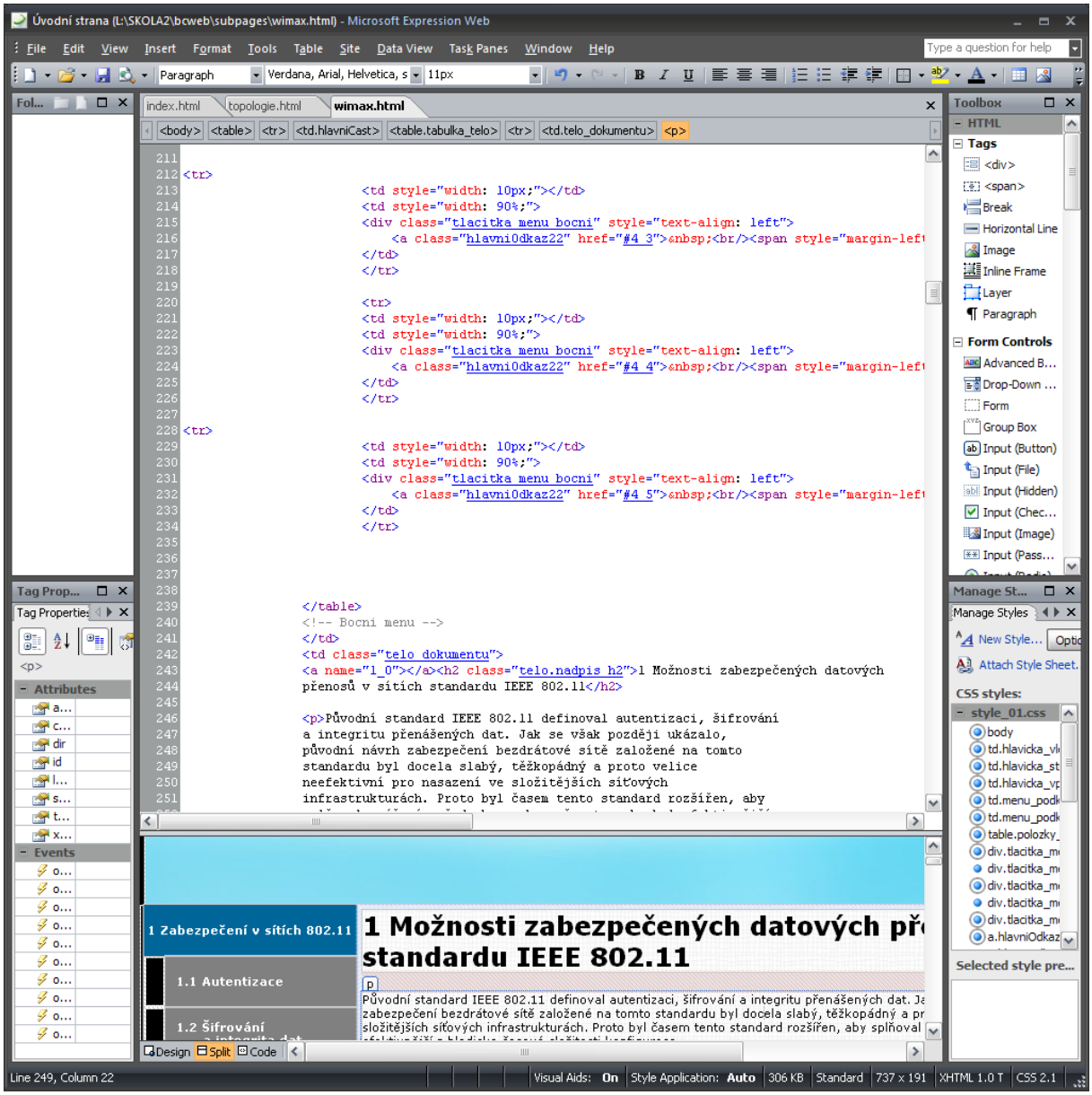
Tab. 1: Shrnutí možných zabezpečení pro různé síťové topologie

Samozřejmě záleží na administrátorovi dané sítě, obzvláště co se týče doplňků zabezpečení, které z nabízených možností využije nebo naopak nevyužije. Například u poskytovatele internetu může být vhodné vysílat SSID z reklamních důvodů.

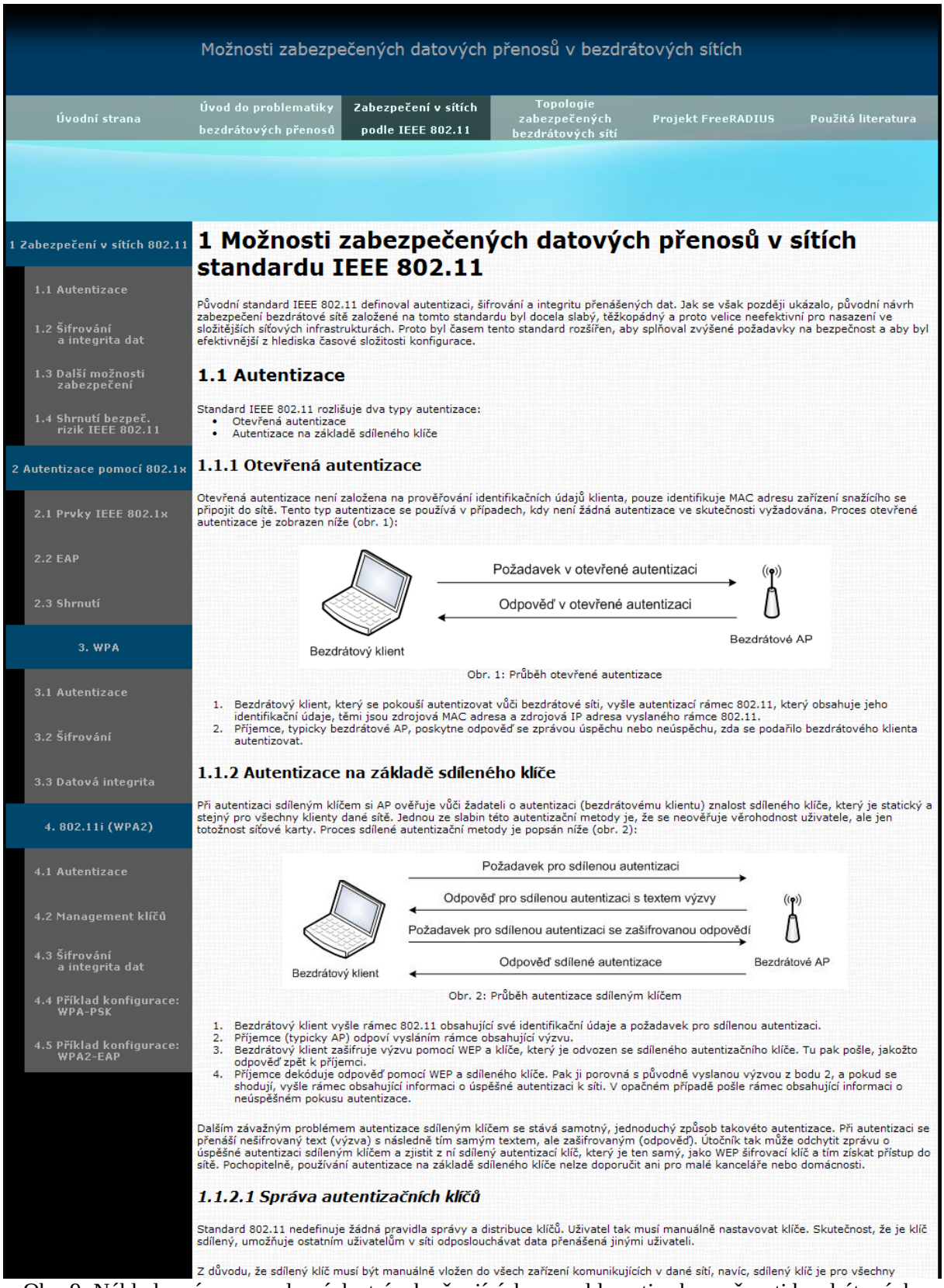
3 Grafické zpracování problematiky bezdrátových přenosů

Součástí této práce je i zpracování této problematiky prostřednictvím webových stránek a animace přibližující možnosti zabezpečení bezdrátových sítí.

Co se týče webových stránek, byly tvořeny pomocí programu Microsoft Expression Web 2. Náhled na tvorbu v tomto web editoru je zobrazen na obrázku níže (obr. 8). Finální vzhled části jedné z webových stránek je zase vyobrazen na další straně (obr. 9).

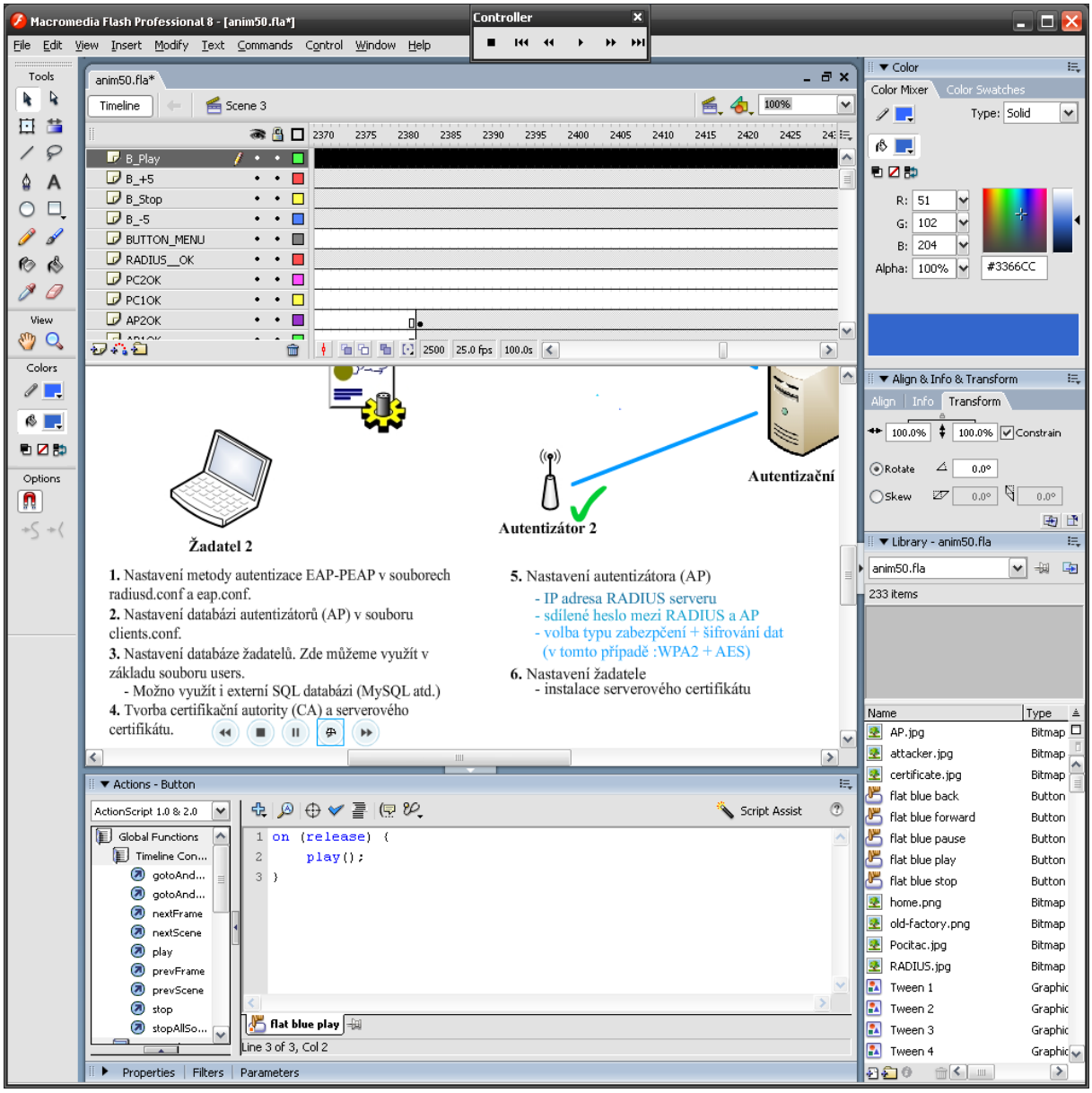


Obr. 8: Ukázka vzhledu vývojového prostředí Microsoft Expression Web 2 pro tvorbu webu.

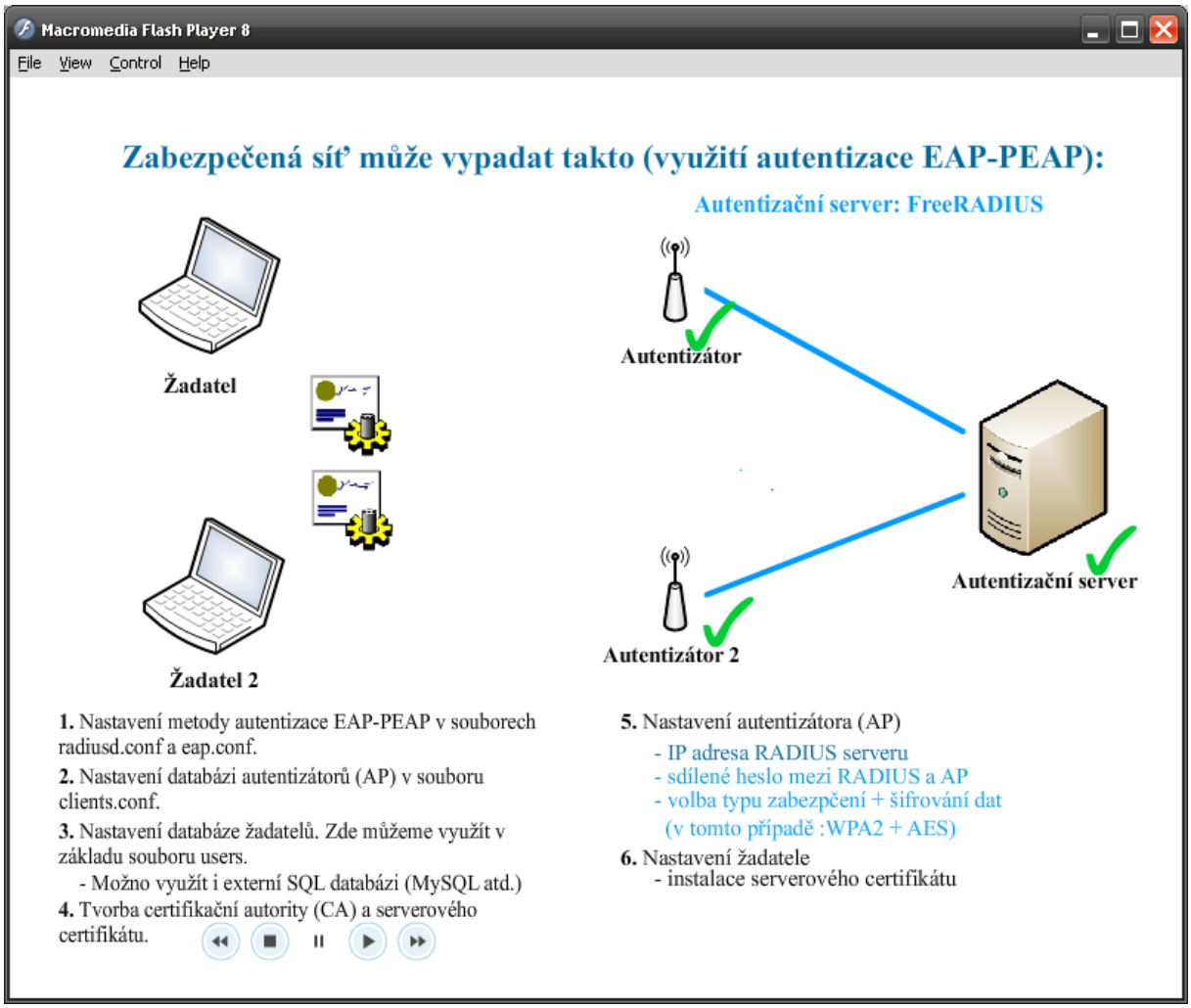


Obr. 9: Náhled na úpravu webových stránek věnujících se problematice bezpečnosti bezdrátových přenosů.

Animace přibližující problematiku zabezpečení bezdrátových sítí byla tvořena pomocí technologie Macromedia Flash. Samotná animace byla tvořena ve vývojovém prostředí Macromedia Flash 8. Ukázka vývojového prostředí je ukázána na obrázku níže (obr. 10).



Obr. 10: Ukázka vývojového prostředí Macromedia Flash Professional 8 pro tvorbu animací.



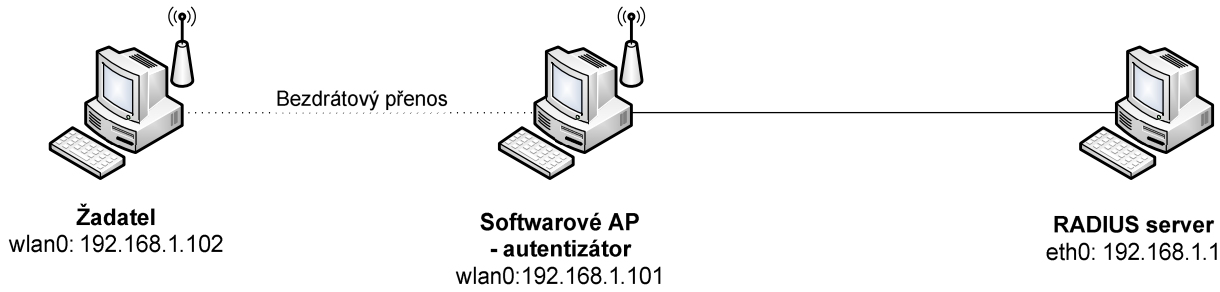
Obr. 11: Ukázka vzhledu výsledné animace vytvořené technologií Macromedia Flash.

Animace včetně zdrojových souborů i webové stránky jsou umístěny na přiloženém CD.

4 Zapojení zabezpečených bezdrátových sítí v laboratoři.

V podmínkách školní laboratoře a mého domova jsem měl možnost si zapojit a tak otestovat bezpečnost bezdrátových přenosů. Volil jsem zapojení od jednodušších – s předsdíleným klíčem až po komplexnější zabezpečená zapojení. Všechna zapojení se týkala sítí dle standardu 802.11 a od tohoto standardu odvozených. U komplexnějších zapojení jsem využil autentizačního serveru FreeRADIUS.

Schéma sítě při použití rozšířených autentizačních metod je zobrazeno níže (obr. 12):



Obr. 12: Schéma zapojení sítě s rozšířenou autentizací

4.1 Projekt FreeRADIUS

Open source projekt FreeRADIUS byl založen v červenci roku 1999 Miquelem van Smoorenburgem a Alanem DeKokem. První alfaverze vyšla již v září roku 1999. V květnu roku 2001 byla vydána verze 0.1. Od té doby je FreeRADIUS pravidelně stabilně aktualizován a nové verze jsou vydávány každých několik měsíců.

V dnešní době se FreeRADIUS řadí k nejpoužívanějším serverům pro autentizaci s podporou mnoha autentizačních metod, viz níže. Denně jeho služeb využívá na 100 miliónů lidí k přístupu do internetu a je využíván ve více než 50 tisících počítačových sítích o velikosti od 10 do 10 miliónů uživatelů [5].

FreeRADIUS podporuje následující autentizační metody:

- PAP
- CHAP
- MS-CHAP
- EAP-MD5, EAP-GTC, EAP-TLS, EAP-TTLS,
- PEAPv0
- LEAP
- EAP-SIM
- další starší typy autentizace

Server podporuje SQL, LDAP, RADIUS Proxy, dělení zátěže a další služby, jejichž popis je nad rámec této práce. Oficiální stránky projektu obsahující i docela spartánskou dokumentaci jsou umístěny na oficiální stránce projektu.

4.1.1 Instalace FreeRADIUS serveru

Instalace AAA serveru FreeRADIUS je velice variabilní. Zvolil jsem si tedy nainstalovat a nakonfigurovat FreeRADIUS server s podporou PEAP a EAP-TLS a se základní databází uživatelů v souboru `users`.

Nainstalovat a zprovoznit FreeRADIUS jsem se rozhodl v linuxové distribuci Debian ve verzi 5.0 (kódové označení „Lenny“). Instalace je sice ve své postatě jednoduchá (klasicky `apt-get install freeradius`), nicméně na základě licenčních podmínek OpenSSL, které nejsou v souladu s Debianem, resp. dodržováním GPL, je nutno si zkompilovat balíčky s podporou EAP-TLS a PEAP.

Začněme tedy aktualizací dostupných balíčků, vytvořením závislostí vzhledem k programu FreeRADIUS a nainstalováním knihovny nezbytné k provozu OpenSSL. Je tedy nutno zadat postupně tyto příkazy:

```
apt-get update
apt-get build-dep freeradius
apt-get install libssl-dev fakeroot
```

Dále je potřeba stáhnout zdrojové kódy samotného programu FreeRADIUS, které upravíme pro podporu PEAP a EAP-TLS. Jako pracovní adresář jsem si zvolil `/usr/src/freeradius` a stáhnul jsem zdrojové kódy:

```
mkdir /usr/src/freeradius && cd /usr/src/freeradius
apt-get source freeradius
```

Nyní, pokud je FreeRADIUS stažen (cca 3MB dat), můžeme provést pár změn v původních nastaveních tak, aby bylo možno použít moduly EAP. K tomu je potřeba nejprve editovat soubor `control` v adresáři `freradius-1.1.7/debian/`. Zde přidáme k řádku `Build-Depends` podporu SSL pomocí knihovny `libssl-dev`. Řádek `Build-Depends` by měl tedy vypadat takto nebo podobně:

```
Build-Depends: debhelper (>= 4.2.32), dpatch (>= 2), autotools-
dev, libtool (>= 1.5), libltdl3-dev, libpam0g-dev,
libmysqlclient15-dev | libmysqlclient14-dev | libmysqlclient-
dev, libgdbm-dev, libldap2-dev, libsasl2-dev, libiodbc2-dev,
libkrb5-dev, libperl-dev, snmp, libsnmp9-dev | libsnmp5-dev |
libsnmp4.2-dev, libpq-dev | postgresql-dev, libssl-dev
```

Dále jsem přidal na konec souboru popis pro nově přidané EAP moduly:

```
Package: freeradius-eaptls
Architecture: any
Depends: freeradius (= ${binary:Version}), ${shlibs:Depends}
Description: eap-tls module for FreeRADIUS server
Debian will not provide a binary version of the rlm_eap_tls.so
library. This
module is required if you want to use EAP/TLS authentication,
commonly used
```

```
for Wi-Fi access points.

Package: freeradius-eappeap
Architecture: any
Depends: freeradius (= ${binary:Version}), ${shlibs:Depends}
Description: eap-peap module for FreeRADIUS server
Debian will not provide a binary version of the rlm_eap_peap.so
library. This
module is required if you want to use EAP/PEAP authentication,
commonly used
for Wi-Fi access points.
```

Dále jsem pak upravil soubor `rules` v adresáři `/usr/src/freeradius/freeradius-1.1.7/debian/`. K řádku `modulepackages` jsem přidal parametry `eap_peap` a `eap_tls`, pak jsem pozměnil i řádek `buildssl`. Finální nastavení parametrů pro `modulepackages` a `buildssl` vypadá takto:

```
buildssl=--without-rlm_otp --without-rlm_sql_postgresql --
without-snmp
modulelist=krb5 ldap sql_mysql sql_iodbc eap_peap eap_tls
```

Nyní bude dobré přidat po-instalační akce pro nově přidaný `eap/peap a eap/tls`. V adresáři `/usr/src/freeradius/freeradius-1.1.3/debian/` jsem tedy vytvořil soubor `freeradius-eappeap.postinst` a vložil do něj tento kód:

```
#! /bin/sh

set -e

case "$1" in
 configure)
       if [ -x "`which invoke-rc.d 2>/dev/null`" ]; then
         invoke-rc.d freeradius reload
       else
         /etc/init.d/freeradius reload
       fi
       ;;
 abort-upgrade)
       ;;
 abort-remove)
       ;;
 abort-deconfigure)
       ;;
esac

#DEBHELPER#
```

Podobně, v tomtéž adresáři jsem vytvořil soubor `freeradius-eaptls.postinst` a vložil do něj následující kód:

```
#! /bin/sh

set -e

case "$1" in
 configure)
       if [ -x "`which invoke-rc.d 2>/dev/null`" ]; then
         invoke-rc.d freeradius restart
       else
         /etc/init.d/freeradius restart
       fi
       ;;
 abort-upgrade)
       ;;
 abort-remove)
       ;;
 abort-deconfigure)
       ;;
esac

#DEBHELPER#
```

Nyní, po přesunutí zpět do pracovního adresáře jsem konečně mohl celý balík zkompilovat tímto příkazem:

```
dpkg-buildpackage -rfakeroot -uc -us
```

Po zkompilování se objevilo v pracovním adresáři několik instalačních `*.deb` balíčků. Nainstaloval jsem tedy tyto z nich a to následujícími příkazy:

```
dpkg -i freeradius_1.1.7-0_i386.deb
dpkg -i freeradius-eaptls_1.1.7-0_i386.deb
dpkg -i freeradius-eappeap_1.1.7-0_i386.deb
```

Zkontroloval jsem instalaci příkazem:

```
ps aux | grep freeradius
```

Proces běží, čili instalace a spuštění se podařilo:

```
freerad 2873 0.0 0.1 46664 2024 ? Ssl 20:10 0:00
/usr/sbin/freeradius
```

V opačném případě je možno spustit FreeRADIUS v debug módu, a tak odhalit problém. Toto se provede parametrem `-X`:

```
freeradius -X
```

4.1.2 Konfigurace FreeRADIUS serveru

Nejprve je nutné upravit soubor `/etc/freeradius/radiusd.conf` a nastavit tyto hodnoty u modulu `mschap`, který podporuje autentizaci MS-CHAP a MS-CHAPv2, které později využijeme. Blok `mschap` v již zmíněném souboru `radiusd.conf` musí mít nastaveny tyto parametry:

```
mschap {
         authtype = MS-CHAP
         use_mppe = yes
         require_encryption = yes
         require_strong = yes
}
```

Následně v bloku `authorize` toho samého souboru je nutno zajistit, aby byly neokomentovány následující položky: `preprocess`, `mschap`, `suffix`, `eap`, `files`.

Blok `authenticate` stejného souboru musí být nakonfigurován takto:

```
authenticate {
  #  MSCHAP authentication.
  Auth-Type MS-CHAP {
mschap
}
#  Allow EAP authentication.
         eap
}
```

Když je kontrola a případná editace konfigurace `radiusd.conf` dokončena, můžeme přidat do souboru `clients.conf`, který je umístěn ve stejném adresáři jako `radiusd.conf`, informaci o klientovi, v mém případě se bude jednat o AP s IP adresou 192.168.1.1, které jsem použil k sestavení této pokusné sítě. Do souboru `clients.conf` tedy můžeme přidat řádky:

```
client   192.168.1.1 {
         secret = Heslo123
         shortname = TestovaciAP
}
```

Nyní, po zkonfigurování souboru `clients.conf` je vhodné upravit soubor `eap.conf` nacházející se ve stejném adresáři jako předchozí editované soubory, tedy `/etc/freeradius/`. Upravení tohoto souboru zajistí serverovou podporu pro PEAP.

Nejprve bude dobré upravit řádek `default_eap_type`. Je třeba změnit, pokud je FreeRADIUS server čistě nainstalován, tuto hodnotu ze základní `md5` na `peap`. Řádek tedy bude vypadat takto:

```
default_eap_type = peap
```

Ve stejném souboru (`eap.conf`), aby server znal cestu k certifikátům, je potřeba odkomentovat blok `tls` a uvnitř odkomentovat také cesty k certifikátům. Uvnitř bloku `tls` musí být nezakomntované tyto položky a celý blok bude vypadat následovně:

```
tls {
private_key_password = whatever
private_key_file = ${raddbdir}/certs/cert-srv.pem
certificate_file = ${raddbdir}/certs/cert-srv.pem
CA_file = ${raddbdir}/certs/demoCA/cacert.pem
dh_file = ${raddbdir}/certs/dh
random_file = ${raddbdir}/certs/random
}
```

Později, po vytvoření certifikátu se upraví i cesty k samotně vzniklým novým certifikátům.

V bloku `peap`, který je v základním nastavení celý zakomentovaný, je nutno odkomentovat následující parametr:

```
default_eap_type = mschapv2
```

Nyní jsem pro otestování systému přidal uživatele do souboru `users` v adresáři `/etc/freeradius/`. Přidal jsem tyto řádky se jménem, heslem uživatele a uvítací zprávou:

```
"jakub"  Cleartext-Password := "password123"
         Reply-Message = "Hello, %u"
```

Po následném restartu FreeRADIUS serveru příkazem `/etc/init.d/freeradius restart` je možno otestovat prozatímní úspěšnost konfigurace příkazem v konzoli:

```
radtest jakub password123 localhost 0 testing123
```

V následném výpisu by se měly objevit tyto řádky, pokud je server nastaven přesně dle mého příkladu konfigurace popisované v předchozích odstavcích:

```
Sending Access-Request of id 153 to 127.0.0.1 port 1812
         User-Name = "jakub"
         User-Password = "password123"
         NAS-IP-Address = 255.255.255.255
         NAS-Port = 0
rad_recv: Access-Accept packet from host 127.0.0.1:1812,
id=153, length=34
         Reply-Message = "Hello, jakub"
```

Pokud vše pracuje jak má, tedy, pokud po otestování FreeRADIUS serveru o několik řádků výše popsaným postupem server běží, je důležité vytvořit si vlastní certifikační autoritu (CA) a také certifikáty pro koncová zařízení, neboť certifikáty uložené v adresářích, na které odkazuje momentální nastavení bloku `tls` v souboru `eap.conf`, slouží pouze testovacím účelům. V následujících odstavcích instalaci a nastavení vhodných nástrojů pro tyto úkony popíšu.

4.1.3 Instalace OpenSSL

Nejprve je nutno nainstalovat OpenSSL, pokud ještě není nainstalovaný a volitelně i PWGen – generátor hesel pro usnadnění práce při vymýšlení komplexních hesel:

```
apt-get install openssl pwgen
```

4.1.4 Tvorba a implementace certifikátů

Po instalaci OpenSSL můžeme využít souboru `openssl.cnf` v adresáři `/etc/ssl/.` Soubor je příkladem konfiguračního souboru pro požadavky výroby certifikátů, a pro tyto potřeby výborně postačuje. Je vhodné si daný soubor nejprve někde zálohovat, než se v něm provedou úpravy. Po otevření onoho souboru `openssl.cnf` je možno změnit parametr umístění, kde chceme vytvořit novou certifikační autoritu. Původní hodnotu parametru:

```
dir   = ./demoCA
```

jsem změnil na:

```
dir   = /etc/freeradius/eap/eapCA
```

Případně lze v tomto souboru změnit i dodatečné údaje, jako stát, kraj, jméno organizace a další. Po fyzickém vytvoření adresáře, jehož jméno jsem zvolil `eap`, dle nastavení v souboru `openssl.cnf`, je vhodná doba pro vytvoření certifikační autority. K tomu je třeba nejprve zkopírovat soubor `CA.pl` z adresáře `/usr/lib/ssl/misc/` do nově vytvořeného adresáře `/etc/freeradius/eap`. Následně tento překopírovaný soubor upravit, konkrétně změnit hodnotu parametru:

```
CATOP="./demoCA";
```

na hodnotu umístění, kde se má vytvořit certifikační autorita, v mém případě:

```
CATOP="/etc/freeradius/eap/eapCA";
```

Certifikační autorita je srdcem celé vytvořené certifikační infrastruktury, proto je zde namístě použít co nejsilnější heslo pro ochranu. Nyní využiju nainstalovaného programu PWGen pro vygenerování hesla. Budu chtít tedy vygenerovat jedno heslo o délce 25 znaků. První řádek je mnou vepsaný příkaz do konzole a druhý řádek je již vygenerované heslo:

```
pwgen 25 1
eogaePo9Reeju2ohsh7ien0th
```

Konečně je možné spustit skript `CA.pl` s parametrem `newca` z adresáře `/etc/freeradius/eap`, který vytvoří certifikační autoritu:

```
./CA.pl  -newca
```

Po spuštění skriptu je nutné odpověďět na všechny otázky a při žádosti o vložení hesla je potřeba vložit ono nově vygenerované heslo, v mém případě pomocí programu PWGen. Po skončení této procedury je nově vzniklá certifikační autorita umístěna v adresáři `/etc/freeradius/eap/eapCA`. Dalším krokem je vytvoření certifikátu pro FreeRADIUS server a jeho podepsání nově vytvořenou certifikační autoritou. Nejprve tedy vytvořím serverový certifikát tímto příkazem:

```
./CA.pl  -newreq-nodes
```

Nyní, pokud bereme v potaz, že v síti se budou vyskytovat koncoví klienti i s operačním systémem Windows XP, je potřeba ještě přidat rozšíření vyžadující si právě tento operační systém od Microsoftu. Soubor s rozšířením je distribuován s balíčkem FreeRADIUS. Stačí ho zkopírovat, soubor se jmenuje

xpextensions, z adresáře /usr/share/doc/freeradius/examples/xpxtensions do adresáře /etc/freeradius/eap.

Nyní využijme klíče naší certifikační autority k podepsání žádosti o certifikát, vložením výše uvedeného, vygenerovaného hesla při požádání:

```
./CA.pl  -sign  -extensions xpserver_ext -extfile
/etc/freeradius/eap/xpextensions
```

Nyní, když jsou všechny požadované certifikáty vygenerované, je potřeba vygenerovat dh pro vyměnu klíčů a nastavit řádnou cestu k vytvořeným certifikátům. K vytvoření dh a náhodných souborů použijeme příkaz:

```
openssl dhparam -check -text -5 512 -out dh
dd if=/dev/urandom of=random count=2
chmod 640 random newcert.pem newkey.pem newreq.pem dh
```

Pokud znovu otevřeme soubor eap.conf v adresáři /etc/freeradius/, můžeme v bloku tls změnit stávající cesty k certifikátům, určené jen pro původní testování, na správné cesty, kde používáme námi vytvořené certifikáty. Vnitřek bloku tls bude tedy upraven takto:

```
private_key_file = /etc/freeradius/eap/newkey.pem
certificate_file = /etc/freeradius/eap/newcert.pem
CA_file = /etc/freeradius/eap/eapCA/cacert.pem
dh_file = /etc/freeradius/eap/dh
random_file = /etc/freeradius/eap/random
```

Dále ve stejném souboru jsem odkomentoval tyto parametry:

```
fragment_size = 1024
include_length = yes
```

Instalace a konfigurace autentizačního serveru FreeRADIUS je nyní kompletní, stačí jej restartovat a certifikáty (/etc/freeradius/eap/eapCA/cacert.pem) zkopírovat ke koncovým klientům. Nyní stačí dokonfigurovat AP pro funkci s FreeRADIUS serverem a koncové klienty, což ukážu dále.

4.1.5 Konfigurace autentizátora pro WEP + 802.1x autentizaci

Konfigurace přístupového bodu je docela jednoduchá, obzvlášť pokud se jedná o hardwarové AP ovládané přes webové rozhraní. Zde stačí nastavit sdílené heslo a IP adresu našeho FreeRADIUS serveru.

Pro Linux poskytuje stejné funkce program Hostapd. Nastavení a jeho možnosti jsou popsány v samotném konfiguračním souboru programu nebo na domovské stránce projektu [6]. Konfigurační soubor má název hostapd.conf a pro funkční nastavení s 802.1x je potřeba mít v konfiguraci zadáno toto (což znemenalo v mém případě odkomentování některých řádků):

```
interface=wlan0
ssid=PrivateNet
ieee8021x=1
```

```
 wep_key_len_broadcast=13 #hodnota 13 pro 104 bitový WEP klíč
(broadcast)
 wep_key_len_unicast=13 #hodnota 13 pro 104 bitový WEP klíč
(unicast)
 wep_rekey_period=300
 own_ip_addr=192.168.1.1 #Adresa AP, na kterém běží hostapd
 auth_server_addr=192.168.1.100 #Adresa našeho FreeRADIUS
serveru
 auth_server_port=1812 #FreeRADIUS server mi běží na tomto
základním portu
 auth_server_shared_secret=secret #Nastavení sdíleného hesla
```

4.1.6 Konfigurace žadatele pro WEP + 802.1x autentizaci

Pro zprovoznění žadatele v Linuxu musí být naistalován balík nástrojů wireless tools podporující wireless extensions a dále také wpa_supplicant, jehož dokumentaci lze nalézt na domovské stránce projetu [7]. Konfigurační soubor programu wpa_supplicant s názvem `wpa_supplicant.conf` vypadá takto:

```
network={
        ssid="PrivateNet"
        key_mgmt=IEEE8021X
        eap=PEAP
        identity="jakub"
        password="password123"
        ca_cert="/etc/cert/cacert.pem"
        phase2="auth=MSCHAPV2"
}
```

Do adresáře uvedeného v nastavení parametru `ca_cert` umístí uživatel certifikát FreeRADIUS serveru. Na mém nainstalovaném a nakonfigurovaném FreeRADIUS serveru se certifikát vyskytuje v adresáři `/etc/freeradius/eap/eapCA/cacert.pem`. Pro zprovoznění této konfigurace stačí spustit wpa_supplicant s rozšířením wext (Linuxové wireless extensions):

```
wpa_supplicant –i eth1 –D wext –c wpa_supplicant.conf
```

Uvedu zde i možnost zprovoznění v operačním systému Windows XP, neboť se očekává, že tento operační systém bude v síti zastoupen v roli žadatele. Příponu certifikátu `cacert.pem` je možno přejmenovat na .crt. Certifikát se tak automaticky asociuje s Crypto Shell Extensions a následným poklepáním na něj se zobrazí průvodce instalace certifikátu. Postup při instalaci je tedy tento:

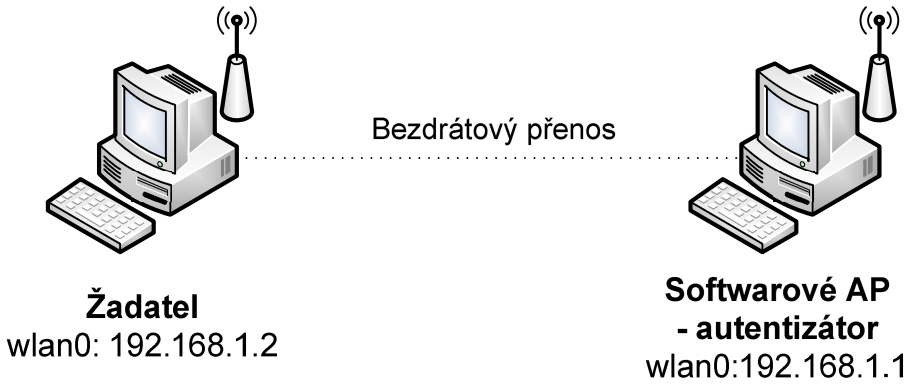
1. V úvodním okně „Certificate“ se zobrazí informace o tomto certifikátu.
2. Po kliknutí na tlačítko „Install Certificate“ se spustí průvodce.
3. V okně průvodce s názvem „Certificate Import Wizard“ je třeba zaškrtnout volbu „Place all certificates in the following store“ a jako „Certificate Store:“ – úložiště certifikátu, vybrat „Trusted Root Certification Authorities“.
4. Po následném kliknutí na tlačítko „Next“ se zobrazí okno se správou o úspěšně nainstalovaném certifikátu.

Nyní můžeme nakonfigurovat bezdrátovou síť žadatele pod Windows XP, aby bylo možné se konečně připojit k síti:

1. Ve vlastnostech bezdrátové síťové karty v záložce Wireless Network je potřeba poklepat na tlačítko „Add…“.
2. V nově otevřeném okně „Wireless network properties“ v první záložce s názvem „Association“ je třeba zadat název sítě (SSID), v mém případě jsem zadal PrivateNet a v panelu „Wireless network key“ vybrat ze seznamu z nastavení „Network Authentication“ volbu „Open“, jako šifrování („Data encryption“) vybrat WEP a zaškrtnout volbu automatické distribuce klíčů („The key is provided for me automatically“).
3. V záložce nastavující autentizaci: „Authentication“ je třeba zaškrtnout volbu „Enable IEEE 802.1x authentication for this network“, čili povolení v této síti ověření IEEE 802.1x. a jako volbu typu rámce EAP („EAP type“) vybrat ze seznamu „Protected EAP (PEAP)“.
4. V této samé záložce po kliknutí na „Properties“ je dále nutno ze seznamu nainstalovaných certifikátů zvolit náš, před chvílí nainstalovaný certifikát a vybrat pro něj autentizační metodu, v mém případě se jednalo o výchozí „Secured password (EAP-MSCHAP-v2)“.
5. Jelikož se můj nakonfigurovaný login a heslo pro 802.1x liší od uživatelského profilu a hesla ve Windows XP, bylo ještě nutné kliknout na tlačítko „Configure“ ve stejném okně a nechat nezaškrtnutou volbu automatického použití přihlašovacího jména a hesla systému Windows („Automatically use my Windows logon name and password (and domain if any).“).
6. Instalace je kompletní a při prvním pokusu o připojení stačí zadat přihlašovací jméno a heslo uložené v souboru users FreeRADIUS serveru v adresáři /etc/freeradius.

4.2 Konfigurace malé bezdrátové sítě s předsdíleným klíčem (WPA-PSK)

Uvažujme síť s jednoduchou architekturou žadatel – autentizátor. Využiji zde právě zabezpečení podle IEEE 802.11i. Nicméně jako příklad u této sítě využiju autentizace WPA-PSK, čili předsdíleného klíče a šifrování dat bude založeno na TKIP Schéma zapojení je zobrazeno na obrázku níže (obr. 13).



Obr. 13: Schéma zapojení pro malou síť s předsdíleným klíčem (WPA-PSK)

4.2.1 Nastavení autentizátora

Nastavení hardwarového AP je triviální, na Linuxu, pokud použijeme softwarové AP, je možno využít programu Hostapd. Příklad konfigurace souboru `hostapd.conf`:

```
interface=wlan0
ssid=PrivateNet
```

```
wpa=1 #Povolení pouze WPA
wpa_pairwise=TKIP
wpa_key_mgmt=WPA-PSK
wpa_passphrase=password123
```

4.2.2 Nastavení žadatele

Na straně žadatele je v Linuxu nutné mít nainstalovaný wpa_supplicant a mít jej nakonfigurován takto:

```
network={
	ssid="PrivateNet"
	proto=WPA
	key_mgmt=WPA-PSK
	pairwise=TKIP
	group=TKIP
	psk="password123"

}
```

V operačním systému Windows XP stačí nastavit oproti předchozí konfiguraci s WEP ve vlastnostech bezdrátového připojení, v záložce „Association“ ověřování k síti WPA-PSK a vybrat šifrování TKIP. Následně zadat síťový klíč a potvrdit změny.

4.3 Konfigurace komplexnější bezdrátové sítě s rozšířenou autentizací (WPA2-EAP)

U bezdrátové sítě s rozšířenou autentizací na základě EAP-PEAP a s využitím WPA2 můžeme mluvit o skutečně robustním a v dnešní době spolehlivém zabezpečení. Schéma sítě je stejné jako při konfiguraci 802.1x + WEP (obr. 12).

4.3.1 Konfigurace autentizačního serveru

Konfiguraci RADIUS serveru – FreeRADIUS, uvažuji stejnou jako v kapitole 4.1.2.

4.3.2 Nastavení autentizátora

Nastavení konfiguračního souboru `hostapd.conf` programu Hostapd na straně autentizátora je podobné jako v konfigurované infrastruktuře s WEP. Síť budu konfigurovat výhradně pro WPA2. Místo parametrů WEP jsou zde tedy relevantní parametry pro WPA2:

```
interface=wlan0
ssid=PrivateNet
ieee8021x=1
wpa=2 #Povolení pouze WPA2
wpa_pairwise=CCMP #Vynucení šifrování CCMP
wpa_key_mgmt=WPA-EAP #Autentizaci bude zajišťovat RADIUS
server
own_ip_addr=192.168.1.1 #Adresa AP, na kterém běží hostapd
auth_server_addr=192.168.1.100 #Adresa našeho FreeRADIUS
serveru
auth_server_port=1812 #FreeRADIUS server mi běží na tomto
základním portu
auth_server_shared_secret=secret #Nastavení sdíleného hesla
```

4.3.3 Nastavení žadatele

Zbývá už jen nakonfigurovat síť na straně žadatele. Konfigurační soubor programu wpa_supplicant, `wpa_supplicant.conf` je nakonfigurován takto:

```
network={
       ssid="PrivateNet"
       proto=RSN
       key_mgmt=WPA-EAP
       eap=PEAP
       pairwise=CCMP
       group=CCMP
       identity="jakub"
       password="password123"
       ca_cert="/etc/cert/cacert.pem"
       phase2="auth=MSCHAPV2"
}
```

V operačním systému Windows XP stačí nastavit oproti předchozí konfiguraci s WEP ve vlastnostech bezdrátového připojení, v záložce „Association“ ověřování k síti WPA2 a vybrat šifrování AES.

Nastavení certifikátů a jejich instalace je stejná jako při konfiguraci 802.1x popisované v kapitolách 4.1.4 až 4.1.6 a to jak pro Linux, tak i pro Windows XP.

5 Závěr

Práce si dala za cíl popsat možnosti zabezpečených datových přenosů v sítích podle standardu IEEE 802.11. Poukázala na jednotlivé zabezpečovací metody, stejně tak jako uvedla příklady konfigurace klíčových síťových prvků, kterými jsou žadatel (koncový klient – většinou uživatel), autentizátor (většinou bezdrátové AP) a v případě použití i autentizační server (většinou RADIUS). Taktéž se snažila vysvětlit princip autentizace, šifrování a integrity datových přenosů u různých zabezpečovacích metod, které jsou součástí standardu IEEE 802.11.

Tato práce by měla přinést užitek zejména lidem zajímajícím se o bezdrátové sítě hlouběji, než obyčejný uživatel. Mou snahou bylo podívat se na zabezpečení bezdrátové sítě hlavně z pohledu administrátora, který má nad celou konfigurací a síťovou infrastrukturou neomezený dohled. Z části se zabývala i příkladem útoků na některé typy zabezpečení a na celkové porovnání silných a slabých stránek jednotlivých zabezpečovacích metod.

Téma zabezpečení bezdrátových sítí je však rozsáhlejší, než stačila pokrýt tato práce. Nezabývala se například bezpečností mobilních sítí, technologií Bluetooth nebo dnes se dynamicky rozvíjející a z bezpečnostního hlediska zajímavou technologií WiMAX (IEEE 802.16), která snad nahradí v dohledné době nestabilní a k rušení velice náchylné Wi-Fi v oblasti poslední míle. Budoucnost dobré bezpečnosti přenosu bezdrátových signálů z komplexního hlediska vidím právě ve formě WiMAX, jako technologie pro poslední míli, ačkoli momentálně se ceny základových stanic pohybují hodně vysoko. Co se týče zabezpečení menších sítí (WLAN) pomocí standardu IEEE 802.11, tak pokud se využije moderních zabezpečovacích technik (IEEE 802.11i), lze tuto technologii považovat za bezpečnou, ostatně pro tyto lokální účely byly sítě WLAN navrženy.

6 Literatura

[1] KLÍMA, Vlastimil. RC4 – Šifra, která míchá karty. *CHIP: magazín informačních technologií*, září 1999, roč. 9, č. 9, s. 42-44. ISSN 1210-0684.

[2] WALKER, R. Jesse. Unsafe at any key size; An analysis of the WEP encapsulation. 1st edition. Intel Corporation, 2000. Dostupný z WWW: <http://www.dis.org/wl/pdf/unsafe.pdf>, s. 3-7.

[3] PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace. 1. vyd. Brno : Computer Press, 2005. 186 s. ISBN 80-251-0791-2.

[4] KOOPMAN, Philip. 32-Bit Cyclic Redundancy Codes for Internet Applications. 1st edition. Pittsburg (USA), 2002. Dostupné z WWW: <http://www.ece.cmu.edu/~koopman/networks/dsn02/dsn02_koopman.pdf > s. 2-9.

[5] *Freeradius – Survey Results*[online], poslední revize 24. 2. 2009 [cit. 2009-05-22]. Dostupné z WWW: <http://freeradius.org/press/survey.html>.

[6]MALINEN, Jouni. *hostapd: IEEE 802.11 AP, IEEE 802.1X/WPA/WPA2/EAP/RADIUS Authenticator*[online], poslední revize 23.3.2009. Dostupné z WWW: <http://hostap.epitest.fi/hostapd/>.

[7] MALINEN, Jouni. *Linux WPA/WPA2/IEEE 802.1X Supplicant* [online], poslední revize 23. 3. 2009. Dostupné z WWW: < http://hostap.epitest.fi/wpa_supplicant/>.

[8]Microsoft Corporation, IEEE 802.11 Wireless LAN Security with Microsoft Windows[Online] 2nd edition, Microsoft Corporation, January 2008. Dostupné z WWW: < http://www.microsoft.com/downloads/details.aspx?FamilyID=67fdeb48-74ec-4ee8-a650-334bb8ec38a9&displaylang=en>.

[9]OpenWRT - Linux distribution for embedded devices[online], poslední revize 29. 3. 2009. Dostupné z WWW:<http://www.openwrt.org>.

[10] LEWIS, Mark. Comparing, Designing, and Deploying VPNs. 1st edition. Indianapolis (USA) : Cisco Press, 2006. Dostupný z WWW: <http://www.ciscopress.com/content/images/1587051796/samplechapter/1587051796content.pdf>. ISBN 1-58705-179-6. What Is a Virtual Private Network?, s. 5-23.